European Parliament

Achieving a sovereign and trustworthy ICT industry in the EU

Fighting cybercrime effectively and ensuring the protection of privacy is critical to guaranteeing the trust of individuals in a digital environment where the number and complexity of cyber threats is growing. The European Union (EU) faces a number of challenges to its goal of achieving a trustworthy and cyber-resilient digital single market: (1) a lack of funding for European cybersecurity companies to scale up; (2) fragmentation of the European cybersecurity industry; (3) strong dependence on non-EU providers; (4) misalignment between public R&D programmes and market needs; (5) regulatory fragmentation; and (6) a lack of common standardisation and procurement requirements across Member States.

Regarding privacy and data protection, even though the EU regulatory framework on such topics is one of the most advanced in the world, challenges remain when it comes to achieving the highest protection for European citizens' personal data. On the global internet, non-EU digital champions transfer personal data to third countries under considerably looser data protection regulation.

The Directive on Security of Network and Information Systems (NIS Directive), the recent cybersecurity package, and the updated Data Protection regulatory framework attempt to solve these problems, although some serious challenges remain.

In this context, establishing policies to increase EU cyber-resilience is crucial to the construction of a trustworthy digital economy and society. The proposed policy options seek to provide an institutional framework where public bodies at the European and national levels can improve cooperation and coordination on tackling cyber threats. They also aim at fostering a healthy and competitive cybersecurity industry in Europe, to reduce excessive dependence on non-EU cybersecurity providers. The policy options also focus on the end users of digital services - an important link in the security chain.

The policies are structured in four groups: institutional policies, market policies, industry policies and demand-side policies. Institutional policies aim at enhancing regulatory remedies to fight against cybercrime while improving coordination between different public administrations. Market policies seek to create a level playing field across Member States, to ease cross-border trade of cybersecurity products and services. Industry policies focus on establishing the right conditions for the European cybersecurity industry to flourish in competition with third country providers. Finally, demand-side policies seek to increase end users' (individuals and companies, mainly SMEs) commitment and knowledge in the cybersecurity process.

Institutional policies

1. **Reinforce the role of EU and national bodies on cybersecurity issues.**

   The cross-border nature of cyber threats makes them difficult to face at country level. However, cybersecurity competences remain at the national level, while the role of the EU bodies (mainly ENISA) is limited to advising Member States and raising awareness among citizens. The NIS Directive and the proposed regulation on the agency (COM(2017) 477) grant new responsibilities to ENISA, although its scope remains quite limited to the areas of advice and assistance. Reinforcing the role of ENISA as an independent and permanent agency, not subject to national interests, would be advisable, as suggested in the proposal for a new regulation on the agency.

2. **Harmonise legislation against cybercrime.**

   Cybercrime is not prosecuted uniformly across the EU, allowing cybercriminals to benefit from more relaxed legislations. Moreover, the borderless nature of cyber-attacks and the principle of territoriality, upon which international law is based, hinders criminal investigation and prosecution, encouraging cyber-delinquent impunity.

The European Judicial Cybercrime Network was launched at the end of 2016 to enhance the exchange of expertise and best practices between the judicial authorities of EU countries. This is not enough. Creating a unified definition of what constitutes a cybercrime, as well as outlining the procedures used to obtain e-evidence in criminal proceedings and which penalties guilty parties will be given to across Member States, could certainly contribute to improving the fight against cyber-criminals.

Market Policies

3. **Unifying public procurement requirements of cybersecurity solutions.**

   Public procurement plays a key role in boosting the cybersecurity industry. However, the variety of public procurement requirements for cybersecurity solutions, mainly certification schemes and standards, across EU countries and among public bodies within the countries, represent a barrier to the development of pan-European cybersecurity companies. This fosters market fragmentation across Europe while limiting the scaling up of European companies.

   The creation of a common set of requirements among the EU and Member State bodies would promote the development of European cybersecurity solutions. The creation of a trustworthy label for European cybersecurity products will further increase the effectiveness of the policy by becoming a common requirement that could benefit Europe-based providers.

4. **Creation of trustworthy labels for European cybersecurity products.**

   The creation of European trust labels for cybersecurity products could benefit the whole ecosystem. Consumers could easily identify trustworthy providers when purchasing cybersecurity solutions, and cybersecurity products with this trust label could be sold across the EU without further adaptations needed in order to meet specific national requirements. Trust labels may also have additional marketing benefits by becoming a powerful tool to signal the quality and reliability of European cybersecurity products.

   The success of the trustworthy labels relies on: (1) developing transparent certification processes; (2) not imposing heavy administrative burdens and (3) being accessible to any company regardless of its size and location.

5. **Harmonise standardisation and certification of cybersecurity products.**

   Currently, the standardisation process of cybersecurity products is booming, as several organisations are trying to set the security specifications for several emerging ICT technologies. The EU should lead the harmonisation of the multiple standards on cybersecurity topics already put in place, as well as establish the definition of a coherent certification framework at European level.

   The joint communication of the European Commission to build a strong cybersecurity for the EU can move forward in the right direction by giving ENISA responsibility for the creation of an EU-wide cybersecurity certification framework, which will establish the procedures to create cybersecurity certification schemes. Although these certification schemes are going to be voluntary, this is an important first step.

Industry Policies

6. **Foster the development of open-source cybersecurity products.**

   Cybersecurity products can be developed as proprietary software or through open-source technologies. The first approach usually yields 'black box' solutions, where customers have no options to inspect how they really work. Open-source software allows the research community to inspect the code for errors and vulnerabilities, continuously improving the reliability and trustworthiness of cybersecurity products. This, however, does not fully guarantee the impossibility of cyber-attacks and it may not be adequate where a certain level of secrecy is required (attack detection and prevention, threat intelligence, etc.). Since the code can be analysed and modified by anyone, it could also be exploited by cyber criminals to develop new vulnerabilities.

   EU bodies can incentivise the development of open-source cybersecurity products by: (1) including 'open-source' requirements on public procurements of cybersecurity and IT solutions, (2) collaborating in open-source software communities to work together on innovative open solutions, (3) clarifying legal aspects related to intellectual property issues, and (4) fostering research based on open-source technologies.

Although open-source is a very interesting option, it should carefully be selected in technical areas avoiding direct competition where the EU has strong proprietary solutions. While open-source solutions can enhance the cyber-resilience of ICT products and services, they do not always provide a competitive advantage to EU providers.

7. **Develop a cybersecurity industrial policy.**

   Current EU industrial policies do not adequately address cybersecurity topics. Neither the European Security Industrial Policy nor the Communication for a European Industrial Renaissance mention this topic among the strategic areas that should be supported.

   It would be necessary to structure all the measures focused on strengthening the European cybersecurity industry in a comprehensive action plan, with clear objectives and a detailed roadmap. The focus should be in areas where the EU is well positioned to be a global leader (i.e. industrial security and cybersecurity for aviation, rail transportation and automotive) and in areas where the EU must be autonomous (i.e. defence, cryptography).

   The industrial policy should be oriented to develop competence centres across Europe where theory and innovation can meet, and views and ideas can be exchanged and evolved in a joint fashion that leads to commercial success. The cybersecurity competence centre network envisaged in the last Commission Cybersecurity Strategy, if well-developed, may be a step in the right direction. The plan should also include support from the EU to promote exports of European cybersecurity solutions and services outside of the EU (particularly to the US, Asia and the EMEA[1] region).

8. **Support the creation of investment instruments focused on the cybersecurity sector.**

   The funding of European cybersecurity companies is focused on early stages (seed capital), and almost disappearing on consolidation and expansion stages. This lack of funding hampers two crucial business processes: (1) marketing activities to improve their visibility, and (2) the adaptation of their products and services to enter new markets. Therefore, it is necessary to design and fund financial instruments covering all stages of business life, especially for a sector that can be observed with reluctance by traditional funding partners (banks).

   The EU has several financial instruments that could be oriented towards the cybersecurity industry. For instance, the European Fund for Strategic Investments (EFSI), a joint initiative by the EIB[2] Group and the European Commission, could allocate funds not only for the general 'digital' sector but also for the cybersecurity sector. It could be made through the creation of a Cybersecurity Investment Platform, which would then finance cybersecurity projects across the EU. This platform not only would be in charge of managing the funds allocated by EFSI, but it would also receive and manage funds from other sources (i.e. public funds from national bodies and private funds) in order to configure several funding instruments according to the needs of the cybersecurity companies.

   Private funds should also play a role in easing industry growth; however, they require a stable and predictable environment to invest in. European bodies could indirectly foster private investments in the sector by harmonising and unifying crucial topics, such as standardisation or labelling, as well as co-investing in mixed fund initiatives and leveraging the investment capacity of institutions such as the EIB.

9. **Foster market-driven research activities.**

   There is evidence showing a misalignment between market needs and research in cybersecurity topics conducted in the EU. The long timescales of EU programme, 3-5 years between conceiving and completing a project, are part of this problem. The European cybersecurity industry tends to think in an incremental way, focusing on building operational capabilities rather than on pursuing long-term strategic planning. Research motivation currently follows a 'science push' instead of a 'market pull' approach and, thus, the EU science results end up being developed by non-EU companies. There is also evidence that the amount of funding available in Europe for R&D activities is scarcely enough to substantially impact the industry.

   Addressing the increasing number of cyber-threats would require better coordination between public bodies in charge of defining research topics and cybersecurity providers that know first-hand the challenges their clients are facing. On top of that we suggest an increase in the amount of funding allocated

[1] Europe, the Middle East and Africa

[2] European Investment Bank

for R&D activities and close supervision of the contributions of private partners outlined in the new contractual public private partnership agreement within the Horizon 2020.

10. Increase the availability of workers in the area of cybersecurity

There is a shortage of professionals in the area of cybersecurity in Europe. This is usually the case in many areas of the digital economy, but it is particularly relevant in the more innovative and evolving fields like cybersecurity.

There are several measures that can be taken to tackle this problem: (1) analyse, together with research establishments and industry, the current needs of cybersecurity-related formal and non-formal education; (2) promote within the industry and training centres lifelong learning programmes for existing professionals aimed at helping establish career paths; (3) raise awareness among students about the career opportunities in the cybersecurity industry and promote cybersecurity studies as a choice at schools; (4) promote cybersecurity studies in universities and vocational training; (5) define a strong EU-wide curriculum and a set of common technical areas by involving every stakeholder (industry, government, military); (6) increase cooperation between education, intelligence and the military in order to share important hard and soft skills and (7) make funding available for qualified EU candidates to study masters and doctoral degrees at universities in Europe or elsewhere.

Demand-side policies

11. Raising awareness of cyber threats among final users (individuals, SMEs)

Cybersecurity is not only about technology, but it is also about people. The way people use digital services has an impact on the potential cyber-attacks they could suffer. Untrained users and those who are less aware of cyber-threats become vulnerable links in the security process.

Training young people in school and launching cybersecurity awareness campaigns, as well as cyber-exercises tailored-made for different target audiences (i.e. minors, teens, parents, trainers, professionals, researchers, c-level executives…), would promote safe and secure online interactions for all citizens regardless of their education or training.

This issue particularly affects individuals and employees of SMEs who both show not only a low level of awareness of cybersecurity topics but also have a general lack of information about such topics. To compound the problem, we have found strong differences depending on the socio-demographic characteristics of the individuals and on the sector and size of the companies. Therefore, we suggest defining different policies depending on these factors. To implement these policies, the European Commission could provide the funding and the basis of the policy, while the national and regional governments and sectorial associations could be in charge of profiling the policies to the specificities of their population and employees. This profiling could be accompanied by a rigorous follow-up from other European bodies. The EU could also lead the development of a single portal to bring together all European cybersecurity tools in a one-stop-shop, which could also offer advice to users on securing their systems, networks and data. Other awareness initiatives, such as the 'European Cyber Security Month', could be reinforced by means, for example, of increasing their advertising budgets to increase the scope of EU citizens they reach.

This document is based on a STOA study on 'Achieving a sovereign and trustworthy ICT industry in the EU' (PE 614.531) published in December 2017. The study was carried out by Iclaves SL (Spain) at the request of the Science and Technology Option Assessment Panel and managed by the Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament.

Authors: Rafael Rivera, Juan Pablo Villar, Carlota Tarín, Arturo Ribagorda, Juan Manuel Estévez, José María De Fuentes and Lorena González. STOA administrator responsible: Zsolt G. Pataki. The study can be found at http://www.europarl.europa.eu/stoa/.