ECS

EUROPEAN CYBER SECURITY ORGANISATION

MANIFESTO

Public-Private Cooperation for Stronger Cybersecurity in Europe

ECSO AND ITS EUROPEAN CYBERSECURITY STAKEHOLDERS COMMUNITY CALL FOR A COMPREHENSIVE PUBLIC-PRIVATE COOPERATION ON CYBERSECURITY IN EUROPE WITH THE FOLLOWING 8 GOALS:

1. Improved resilience for the increased digitalisation of society

We, the European cybersecurity stakeholders, while considering the growing digitalisation of the society, we will work with all the European cyber security community to efficiently drive the development, implementation and use of trusted and resilient solutions.

2. Technological, Societal, Economic and Political Issues. Different views, one challenge: cyber threats

We will tackle cyber threats with a holistic approach as all issues, be they Technological, Societal, Economic or Political, are linked and often interdependent.

3. A comprehensive European cybersecurity strategy and industrial cybersecurity policy, supported by a stronger digital education and awareness

We call for a comprehensive European cybersecurity strategy and the implementation of a European cybersecurity industrial policy, including R&I, as proposed by ECSO in its working groups. This should be supported by an adequate local, regional, national and European coordination.

4. EU industry competitiveness driven by European stakeholders supported by targeted investments

We must build cybersecurity and competitiveness upon a commonly agreed vision for cybersecurity in Europe with adequate level of targeted investments, while encompassing our core values to protect data and privacy.

5. Increased European Cybersecurity Strategic Autonomy for Cybersecurity

While considering the importance of preserving national security interests, we should consider the possibility to establish a cooperation geared to achieve an effective degree of European cybersecurity autonomy to commonly protect our economy, society, market and infrastructures from cyber threats.

6. Trusted supply chains

We recognise the need for increased trust at European level of strategic components, solutions and services throughout the supply chain and hence to develop European cybersecurity standards and certification of components, systems and services. The main objective is to establish trusted supply chains at European level, also via international cooperation.

7. From National cooperation to EU approaches: the European Cybersecurity Community

We recognise the need to build up the Cybersecurity Community at national and European level, fostering coordination across competent stakeholders and sectors to link them in a European Network.

8. Future EU cybersecurity organisation and evolution of ECSO in an enhanced Public-Private Cooperation

We stress that the Public-Private cooperation started in ECSO should be continued, considering common objectives, while reducing unnecessary fragmentation or duplication of approaches.

RECOMMENDATIONS

TO SUPPORT THE ACHIEVEMENT OF THE 8 GOALS IN THIS MANIFESTO

1. Increased resilience for the increased digitalisation of society

We, the European cybersecurity stakeholders, while considering the growing digitalisation of the society, we will work with all the European cyber security community to efficiently drive the development, implementation and use of trusted and resilient solutions.

The digitalisation of society is increasingly pervasive. We are only at the beginning of the digital transformation and are far from understanding the advantages and the opportunities, but also all the potential threats, that comes with it.

Considering this growing digitalisation of society, the dependence on IT systems from all aspects of life and the fast evolving and increased number of cyber threats, we will work with all European stakeholders for a stronger societal and economical resilience to cyber threats.

The protection and support to the digital transition should go hand in hand with the evolution envisaged for the climate-neutral economy in a new Circular Economy.

2. Technological, Societal, Economic and Political Issues. Different views, one challenge: cyber threats

We, the European cybersecurity stakeholders, will tackle cyber threats with a holistic approach, as all issues, be they Technological, Societal, Economic or Political are linked and often interdependent.

Cyber threats heavily impact the European economy and its citizens. This concerns not only technical problems, but also generates political, societal and economic issues.

Cybersecurity, cybercrime and cyber defence all revolve around one challenge: cyber threats! The difference lies in the perpetrators and the potential victims. Europe should be a global leader in preventing and countering these threats: this should be understood and supported at all levels, in particular at the political level.

We have recently seen that the unproper use of data and information from social media as well as dissemination of fake news can endanger the stability of our countries. Governments, the private sector and citizens should be well aware and prepared to prevent or counter these threats.

3. A comprehensive European cybersecurity strategy and industrial cybersecurity policy, supported by a stronger digital education and awareness

We, the European cybersecurity stakeholders, are calling for a comprehensive European cybersecurity strategy and the implementation of a European cybersecurity industrial policy, including R&I (Research and Innovation), as proposed by ECSO in its working groups. This should be supported by an adequate local, regional, national and European coordination.

A comprehensive European cybersecurity strategy supported by a cybersecurity industrial policy, with an increased and structured cooperation at European level, will make Europe a global leader in the domain.

The implementation of a European cybersecurity industrial policy must, through the harmonisation of measures, lead to an enhanced protection of the EU digitalisation, higher competitiveness and stronger digital autonomy (strategic capability management and data ownership and management).

a. A European cybersecurity industrial policy should be formally established upon a continuous enhancement and scaling up of the initiatives stemming from the public-private cooperation piloted by ECSO: standardisation, certification and trusted supply chain, financing and higher harmonised investments, market knowledge, cooperation with users for vertical needs and information exchange, support to SMEs and regional/ local aspects, innovation, education and training, R&I, etc.

b. This policy should allow to develop and maintain a strong, resilient and competitive European industrial and academic ecosystem, while increasing our technological leadership and strategic autonomy for cybersecurity.

c. Cybersecurity must be recognised as an industrial sector, sustained by an industrial policy for Europe, supported by adequate and targeted investments for increased EU competitiveness.

d. A European global leadership in the cybersecurity market would be achieved through a comprehensive European cybersecurity strategy built upon a "predict-prevention, protection, detection, respond" approach as the rationale for a sound investment strategy, based on commonly agreed R&I priorities for an increased strategic autonomy. The EU cyber strategies have so far been focusing mainly on the predict and protect pillars so there is a need to widen the political spectrum to include a focus on detect and respond.

e. European cybersecurity solutions should be effectively deployed at national, regional/ local (city) level and should be driven by smart specialisation.

f. Well informed European citizens and decision makers and highly trained cybersecurity professionals are needed. Increased Awareness is a key component to implement and use appropriately digital innovations. Digitalisation has increased job opportunities which are currently not entirely met.

g. Education on cyber threats, cyber solutions and the possibilities for new jobs in cybersecurity and the ICT sector in general following the digital transformation should start in all Member State from the earliest age.

h. While addressing the need for a larger number of experts in the cybersecurity domain, we should not forget the contribution of women: their enhanced participation should start as early as possible, from school level and their treatment at professional level should be fair and proportional to their job competence.

This approach would help the harmonised growth of our cybersecurity ecosystem at regional, national and European level, in order to reduce fragmentation and efficiently support our industry, support our SMEs, coordinate our R&I and facilitate the implementation of agreed measures and legislations.

4. EU industry competitiveness driven by European stakeholders supported by targeted investments

We, the European cybersecurity stakeholders, must build cybersecurity and competitiveness upon a commonly agreed vision for cybersecurity in Europe with adequate investments, while encompassing our core values to protect data and privacy.

Europe benefits from an innovative industry base (including a substantial portion of SMEs), great scientific knowledge, and advanced R&I capabilities. We should leverage and build upon these assets.

Yet, the European cybersecurity industry suppliers are still not sufficiently competitive at global, and often also, at national level. Furthermore, European global leaders in different economic sectors need to be protected against cyber threats to remain competitive with the increasing digitalisation of their manufacturing environment and offer.

We should build a level playing field throughout the digital single market and contribute to the work addressing the distortive effects of foreign subsidies.

Today, there are still too few European champions in this sector: they should increasingly be the drivers of the European IT and cybersecurity economy.

The participation of users in our dialogue, be they public or private, is fundamental. Yet, effective cooperation with users at European level is still a challenge as there are different interests and often different national approaches. The potential reputational damage is perceived as a threat.

SMEs, which widely populate our European landscape, are also insufficiently supported. The role of SMEs is very important, as they constitute a large part of the national fabric and are the main drivers of innovation. Stronger support to SMEs, be they suppliers or users, should be considered in the future plans of the European Commission in a more efficient approach with the envisaged new SME strategy to help them scale up and expand, including through improved access to finance.

Research Centres and Universities should be more closely linked to the market and the industry (users/ suppliers) to better exploit their innovation capability and keep their competence in Europe.

Initial strategic and innovative investment mechanisms for increased competitiveness must be well targeted, strengthened and increased, to match the levels of other global players and ensure a certain level of digital autonomy. These investments must be used strategically to develop European capabilities and pave the way to encourage private investments in innovation and SMEs. National and European funds should be well coordinated with private investments to achieve synergetic effects.

We need to invest in strategic innovations which will put European industry among the future leaders: Artificial Intelligence, Quantum Computing, Distributed Ledger Technologies (including Blockchain), Secure IoT for commercial and industry applications; microelectronics (chips and their implementation); Data sharing and use (Cloud/Fog/Edge); 5G and increased mobility while preparing the future 6G to be possibly deployed in 2030. The developments should be done encompassing our core values to protect data and privacy. The future starts today.

5. Increased European Cybersecurity Strategic Autonomy for Cybersecurity

We, the European cybersecurity stakeholders, while considering the importance to preserve national security interests, should consider the possibility to establish a cooperation geared to achieve an effective degree of European Cybersecurity Autonomy to commonly protect our economy, society, market and infrastructures from cyber threats.

Each European country has the prerogative to control its security and implementation of adequate measures, but we will only be able to face these threats through a real cooperation across nations.

Cybersecurity, and IT in general, is still not sufficiently considered as a real priority by the political and the economic sector. Investments are not sufficient. Yet, IT is at the heart of digitalisation in every sector. If Europe does not master strategic Information Technologies and their security, it will be relegated to a follower role and will not have the effective control of its security and the development of its economy.

While preserving sovereignty, national governments and the E. Parliament should foster the growth of a Digital Europe and of stronger European cybersecurity solutions, while increasing citizens' trust in innovations.

An increased cybersecurity autonomy at European level could be developed starting from national needs for (cyber) security, building it up at European level into a strong cooperation across countries with substantial and focussed public – private investments. A European network of public and private stakeholders can then be used for its implementation.

6. Trusted supply chains

We, the European cybersecurity stakeholders, recognize the need for increased trust at European level of strategic components, solutions and services throughout the supply chain and hence to develop European cybersecurity standards and certification of components, systems and services. The main objective is to establish trusted supply chains at European level also via international cooperation.

To effectively protect its Digital Single Market, Europe should ensure stability of growth by boosting the competitiveness of its industry and making sure that products, services and systems procured by users and operators in Europe follow commonly agreed standards and certification mechanisms to be deemed trustworthy (promote "IT Made in Europe"). The establishment of a European Certification Framework is a first step in this direction.

A label promoting "Cybersecurity Made in Europe" could also be adopted at European level, as the one proposed by ECSO, in cooperation with national cybersecurity organisations for those companies that effectively follow certain criteria for European trust.

While looking for an increased digital autonomy in the IT sector, and in particular for cybersecurity, Europe must realise that cyber threats are global and supply chains for digital solutions are fed by the global market. While strengthening the European cybersecurity community, we have to keep open the dialogue, cooperation and exchange with international stakeholders looking for the possible establishment of an international public-private dialogue and cooperation on cyber threats and trusted solutions, in a fair and democratic governance, under reciprocity rules.

EU State aid rules and public procurement should support strategic investments where there are market failures and the need to strengthen European value chains (as identified in the IPCEI initiative).

7. From National cooperation to EU approaches: the European Cybersecurity Community

We, the European cybersecurity stakeholders, recognize the need to build up the Cybersecurity Community at national and European level, fostering coordination across stakeholders and linking them in a European Network.

While developing European views, national and local issues should not be forgotten. National coordination, also through local associations and regions, is fundamental for an effective and sustainable market deployment.

Member States, through their national cybersecurity agencies, should support the deployment and procurement of trusted and innovative European products, services and systems with adequate strategic procurement policies.

National public administrations are the driving forces at national level and are coordinating their actions with the private sector across the different vertical sectors.

National public administrations cannot face cyber threats alone. They have to exchange information with the private sector on threats, with critical infrastructure or service providers, on possible solutions with technology providers, be they large companies, SMEs or research centres and universities.

Only in an efficient public-private cooperation can we successfully face global cyber threats and bring innovation to effective market implementation and use. Each country is developing a special relationship between its public and private sector at regional or national level and with the creation of national CERTs, the transposition at national level of the NIS Directive and, where possible, the creation of national certification centres will provide an improved structure to face these threats.

The gathering of these national public and private stakeholders at European level will strengthen the Community already built up by ECSO.

At European level, ECSO has developed and is strengthening every day a new form of effective public-private cooperation. The two approaches, national and European, can be linked and the experience of ECSO can benefit all countries. Also, the competence and common trust developed in ECSO (including the NAPAC for public administrations) can be used to provide support to the working groups of the envisaged European Cybersecurity Centre and in linking national approaches, including supporting the coordination of the Network of National Coordination Centres.

This European Cybersecurity Community should be based upon European stakeholders but should also allow cooperation with third parties to build trusted supply chain and international fight against cybercrime.

8. Future EU cybersecurity organisation and evolution of ECSO in an enhanced public-private Cooperation

We, the European cybersecurity stakeholders, recognize that the public-private cooperation started in ECSO should be continued, considering common objectives, while reducing useless fragmentation or duplication of approaches.

We live in an increasingly complex IT-based society where stakeholders' interests can vary. Yet, the fight against cyber threats should be a common goal. ECSO has started to reduce fragmentation in Europe with its public-private dialogue and cooperation: we should be careful not to develop new structures and processes that will increase fragmentation or duplications and bring frictions within the European cybersecurity Community.

ECSO, with its innovative Public-Private Partnership, gathering all the different categories of stakeholders, has undertaken a major step forward in the dialogue and cooperation across all the different sectors and industrial policy issues.

ECSO has been designed for the purpose of the cPPP and must therefore evolve in its structure, membership and governance to fit with the objectives, challenges and legal parameters of the new tools set up by the proposed Regulation on the ECC, the Network and the Community. ECSO members are fully committed to move forward together in this direction provided that the openness, collaborative spirit and result-driven approach of the organisation be preserved.

The future European cybersecurity ecosystem and related measures should allow European cybersecurity solutions to be effectively deployed at national, regional / local level with adequate supporting instruments and make Europe a global leader in the domain.

We need to put together initiatives and work together between national public administrations, EU institutions and the private sector. This is what ECSO has tried to do and this is what we should do in the future.

The European Cybersecurity Community can be further developed in a spirit of solidarity, in an enhanced Public-Private Partnership at European level, with the support from ECSO as leader of the European Community.

ECSO should be one of the cornerstones for the construction of the future European governance in the cybersecurity domain, leveraging upon strategic European assets. We are confident in the willingness of all stakeholders to continue this excellent initiative and have ECSO continue to represent the European cybersecurity Community at large and be the main non-institutional side of the tools and mechanisms that the ECC and the Network aim to build.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

If you have any question you would like to ask please contact us

10, Rue Montoyer
1000m Brussels
BELGIUM

+32(0) 27770258
secretariat@ecs-org.eu