EUROPEAN CYBER SECURITY ORGANISATION

RECOMMENDATIONS TO THE EUROPEAN COMMISSION AND THE EUROPEAN PARLIAMENT

For a cyber resilient Europe with increased digital autonomy, restoring sovereignty and supporting the socio / economic development - JANUARY 2020

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Recommendations

1. Foster cooperation between all stakeholders in Europe (public and private, citizens, professionals and decision makers) to develop our cybersecure digital ecosystem protecting the growing digital transformation
2. Develop an EU Vision on Cybersecurity and a comprehensive approach for cybersecurity
3. Further develop a comprehensive EU Cybersecurity Strategy and approach
4. Implement a European cybersecurity industrial policy
5. Develop skills and training to satisfy increasing job needs, education / cyber – hygiene for youth and citizens, awareness for professionals and decision makers
6. Recover a higher level of sovereignty and support the socio / economic development through an increased digital autonomy in Europe
7. Develop a European legislative and regulatory cybersecurity framework for sensitive applications
8. Combine higher Public and Private Investments in innovative approaches directed towards Research, Capability Development and Capacity Building
9. Develop trusted supply chains and level playing field
10. Develop the Next Generation Public Private Cooperation strengthening the European Cybersecurity Community to support the implement of these recommendations: ECSO 2.0

PROTECTION OF THE EU DIGITAL TRANSFORMATION ➔

EU VISION FOR A EUROPEAN CYBERSECURITY ECOSYSTEM BASED ON EU VALUES

Comprehensive EU Cybersecurity Strategy and Approach
EU Cybersecurity Industrial Policy
Education, Training / Skills and Awareness

SOVEREIGNTY RECOVERY SOCIO/ECONOMIC DEVELOPMENT

INCREASED DIGITAL AUTONOMY

EU Legislations & Regulations
Public and Private Investments in Research, Capability Development and Capacity Building
Strategic Alliance & Partnership for Trusted Supply Chains

NEXT GENERATION PUBLIC PRIVATE COOPERATION: ECSO 2.0

1. Foster cooperation between all stakeholders in Europe (public and private, citizens, professionals and decision makers) to develop our cybersecure digital ecosystem protecting the growing digital transformation

Digital Transformation is only at the beginning: it brings wealth but also causes Technological, Societal, Economic and Political Issues as well as loss of Sovereignty on Data. This process already has a major direct impact on our societies, economies and political life.

Due to global digitalisation, we find ourselves interconnected across countries, with dependencies which are imposed by circumstances largely beyond our control. **Dependencies throughout the digital transformation and the supply chain can challenge the sovereignty of EU countries impacting national security, citizens and industry with the erosion of control on data**.

Cybersecurity should protect the growing digital / cyber space from regular and increasingly sophisticated attacks. Therefore, it is essential to **improve the resilience of the digitalisation process at local/regional, national and European level.**

Information Technologies (IT) are at the heart of digitalisation in every sector and of the socio / economic development in each country. Yet, cybersecurity, and IT in general, are still not sufficiently considered as main priorities by the political and the economic sector and the level of investments remain insufficient.

If Europe will not master strategic IT innovations and cybersecurity solutions will be relegated to a follower role and could not have the effective control over the protection of its digital transformation and its data.

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

Because of the high level of complexity and dependence of our society, EU Member States (MS) cannot recover a higher level of sovereignty alone. **A higher level of digital autonomy** and the development of an efficient **European cybersecurity ecosystem are only possible through a collective effort across EU MS**.

To **recover and preserve the sovereignty aspects of digitalisation**, local/regional authorities, national governments and European Institutions should foster the growth of a Digital Europe and of stronger and trusted European cybersecurity solutions, while increasing citizens' awareness, education and encouraging (public-private) multi-stakeholder collaboration across sectors and across local/regional, national and European levels.

2. Develop an EU Vision on Cybersecurity and a comprehensive approach for cybersecurity

Europe cannot undergo its digital transformation while facing evolving threats without being sufficiently prepared. Therefore, Europe needs a **comprehensive approach for cybersecurity** to protect its society, its democracy, its sovereignty, its economy.

The development of a **European cybersecurity ecosystem** must be promoted through a **commonly agreed vision at European level based upon our EU values** and deployed at local/regional and national level, leveraging upon:

a) A **comprehensive** and regularly updated **European cybersecurity strategy** leveraging upon national strategies.

b) A **European cybersecurity industrial policy**, to support the EU industry and its competitiveness.

c) Policies, initiatives and programmes enabling **awareness of citizens, decision makers and operational experts as well as boosting education and skills** to meet the growing job market needs.

3. Further develop a comprehensive EU Cybersecurity Strategy and approach

A European Cybersecurity Strategy was issued by the E. Commission in 2013 and updated in 2017. Yet, it is still composed by singular elements (“bricks”) which do not give the full picture (“vision”) of the future European cybersecurity ecosystem.

In particular, the **interaction and operational cooperation between the public and the private sector based on a multiscale (from local to European level) governance approach**, is not sufficiently developed. This is a critical issue to be solved, if we want to reduce the market fragmentation and reach the needed synergies to protect our society and economy.

Local / regional needs should be duly considered, as they often carry challenging issues to be integrated at national level and are the concrete expression of the society and of the market. Regional smart specialisation strategies (S3) could be applied to tackle these issues.

The **different technology aspects of the digital transformation should also be considered in a comprehensive approach**, as digital solutions are increasingly creating interdependencies across applications and threats (e.g. the interlink between 5G, IoT, cloud / edge, AI, etc. and the respective cybersecurity issues).

4. Implement a European cybersecurity industrial policy

A **European cybersecurity industrial policy** should be formally established upon a continuous enhancement and **scaling up of the initiatives stemming from public-private cooperation** (similar to those already implemented by ECSO): standardisation, certification and trusted supply chain, financing harmonised investments, market knowledge, cooperation with users for vertical needs and threats information exchange, assistance to fast responses in crisis situations, support to SMEs and local / regional aspects, innovation, education and training, R&I, etc.

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

Particular attention in such an industrial policy should be dedicated to **SMEs (users and suppliers) of cybersecurity solutions and services**. Larger EU funding dedicated to European SMEs should not only help the development of start-ups or innovation, but should also financially support EU users / integrators to buy from EU SMEs, thus helping the development of a trusted EU supply chain and a sustainable EU digital single market.

5. Develop skills and training to satisfy increasing job needs, education / cyber – hygiene for youth and citizens, awareness for professionals and decision makers

The digital transformation will radically change the needs of the job market. Certain jobs will disappear, others will be created. Digitalisation has already increased the number of job opportunities in IT / cybersecurity and vacancies are currently far from being covered. Highly trained cybersecurity professionals but also other non-STEM specialists working in the digital domain are needed to support this evolution.

Education and cyber hygiene on cyber threats, cyber solutions and the possibilities for new jobs in cybersecurity and the ICT sector in general, should be implemented in all Member States (MS) from the earliest age. Non-EU countries do not usually have cybersecurity curricula at public schools: this could create an incomparable advantage for us compared to other geolocations.

Indeed, **Europe has outstanding software and soft skill competences** in the cyber domain which constitutes one of the fastest growing economy segments. Yet, the lack of an easily accessible and well developed EU market (particularly in East Europe) means that US and Far East tech solution providers are the largest beneficiaries of such potential, while we should instead be using such skills for building “our” capacity.

While addressing the need for a larger number of experts in the cybersecurity domain, we should not forget the **contribution of women**: their interest and participation from school level should be enhanced and their fair promotion at professional level should be encouraged.

Beyond professional skills, well **informed European citizens and increased awareness of operators and decision makers** are key components to implement and use digital innovations appropriately, while being able to efficiently and rapidly respond to threats.

6. Recover a higher level of sovereignty and support the socio / economic development through an increased digital autonomy in Europe

Maintaining a good level of sovereignty, despite the challenges of the digital transformation, means increasing the level of strategic digital autonomy in Europe.

Recovery of a higher level of sovereignty through an increased digital autonomy in Europe must be based on:

a) Common **legislative and regulatory measures** to support the implementation and uptake of strategic European solutions (including, for instance, preference when possible of European products, solutions and services in case of sensitive applications).

b) An **adequate level of investments and innovative investment mechanisms** on identified needs for the development of strategic capabilities (technologies, solutions, services, skills) for increased European Digital Autonomy, in some cases supported by European and/or procurement policies (capacity building), to ensure a harmonised and well-orchestrated European market (demand / supply).

c) Build-up of **strategic alliances with several like-minded countries / suppliers** to develop a sustainable and trusted supply chain for those components / systems / services that Europe will not produce and sustain European cybersecurity solutions abroad. European Certification of the different elements from Europe and abroad will allow the development of trusted Supply Chains and support a trusted digital transformation.

7. Develop a European legislative and regulatory cybersecurity framework for sensitive applications

To increase the digital autonomy of Europe we need **appropriate European rules / regulations to shape the ecosystem and drive the harmonised implementation of those strategic solutions developed in Europe or externally purchased when certified as trustworthy**.

Without such EU legislations there is the risk of creating weak points in the supply chain. Different ways of transposing directives could lead to potential weaknesses in case of interdependencies. For this reason, regulations should be preferred, when possible.

The EU should be able to produce and master those technologies that control very sensitive / strategic data. **The use of such technologies could be regulated, making mandatory the use of certified solutions for sensitive applications** (e.g. art. 12 of the proposed DEP Regulation) hence establishing the criteria (according to sensitiveness of data management) for "make or buy"**.**

EU regulations could consider preferential implementation and use of European solutions already available, thus immediately supporting EU industries and the competitiveness of their offer.

Each country is implementing the latest EU legislations / recommendations, developing a special relationship between its public and private sector at regional or national level. For instance, the creation of national CERTs cooperating with the private sector and the transposition at national level of the NIS Directive will contribute to better facing cyber threats, with the promotion of harmonised cybersecurity requirements for key devices (e.g. IoT) and services related to critical infrastructures and, where possible, the creation of certification centres tackling European requirements.

A stronger public – private cooperation should also be envisaged to respond to crisis situations, developing operational links across Europe, also considering a **possible evolution of the NIS Directive** to make it closer to effective operational / market needs.

8. Combine higher Public and Private Investments in innovative approaches directed towards Research, Capability Development and Capacity Building

Larger and focused investments are needed to support the fast pace of digitalisation and master strategic solutions. Investments must leverage not only on public investments but must also find synergies with private investments.

The **identification of gaps/areas where strategic digital autonomy is needed**, **along with qualified risk assessment**: this would be the first step to design, finance and implement appropriate common mitigation measures, building up an increased digital autonomy.

Public administrations (at local/regional, national or EU level) may consider that identification of priorities for investment should be defined, as in other security or defence sectors, mainly by the public sector, as it is a matter of "sovereignty" and when it comes to security, markets are often led by public administrations (e.g. law enforcement). Yet, cybersecurity is a highly complex market composed (in majority) by important private customers / users.

Currently foreseen investments from the public sector (EC, MS) in Europe on cybersecurity will not be sufficient alone to reach an adequate level of strategic autonomy (i.e. trusted EU solutions).

These investments are only “seed money”, useful to stimulate, gather and initiate cooperation among public and private stakeholders as well as help to mature the digital ecosystem.

The risk is that public money, invested without enough support from the private sector, will only feed traditional approaches without sufficiently impacting on the ecosystem / market. Without enough interest from industry on the proposed priorities, EU budgets could even remain unused, giving the wrong perception that there is no need for investments.

It is **only by linking public money with private investments in an effective public-private co-operation that concrete results and an increased level of digital autonomy to strengthen our sovereignty can be achieved**!

A suitable governance for engaging public money (national and European funds) and creating innovative synergies with a significant private sector contribution, should be considered.

The list of needed technologies is long and rapidly evolving with the changing market needs. The challenge is to **agree on common priorities for investments** (to effectively reach “critical mass of investments”) **that can be validly financed with the available resources, to increase European autonomy and global competitiveness**, avoiding useless duplications and creation of multiple competitors within Europe. Europe should build its own leaders in areas where it has competence, concrete advances or in really innovative solutions.

Only European industry can provide technologies for an increased level of digital autonomy to strengthen our sovereignty, and without the effective engagement and financial support from the EU industry (users and suppliers), there will never be European digital solutions nor effective sovereignty in EU MS.

Indeed, strategic and innovative co-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**.

We need to **invest in strategic innovations** which will put European industry among the future global champions: **Artificial Intelligence, Distributed Ledger Technologies (including Blockchain), Secure IoT for commercial and industry applications; Microelectronics (advanced chips and their implementation in strategic innovations); Data sharing and use (Cloud/Fog/Edge); 5G and increased mobility while preparing the future 6G; Quantum Computing and its Network Infrastructure; Cryptography for the post-quantum era** to be possibly deployed by 2030. The developments should be done encompassing our core values to protect data and privacy.

A **comprehensive approach for investments, from R&D to Market**, should be developed, to avoid dispersion of resources and effective use of strategic innovation in market applications

a) **Fundamental research**: R&D funds for basic / disruptive technologies (Horizon Europe - HE - for TRL up to 5)

b) **Capability development** (in particular for recovery of sovereignty): Convergence of public and private funds for capability development and important tools (e.g. Digital Europe Programme - DEP and HE for TRL 5 to 8); private investments or State Aids (e.g. Important Projects for Common European Interest - IPCEI)

c) **Infrastructure capacity building**: Convergence of EU funds (DEP, Connecting Europe Facility - CEF, other), MS funds and private funds for infrastructure at EU and MS level

d) **Operational capacity building / short term needs for economy and society - national security**: Structural / regional funds & private funds

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).

Lastly, despite cyber threats being global, it should be noted that **the level of digital maturity and the perception of needs are different across Europe**. Smaller states without large national companies in the IT sector and **East EU countries are suffering by the lack of European investments** in the cybersecurity domain and are **largely dependent on third country solutions** for capacity building, while offering often a high level skill capacity at national level.

9. Develop trusted supply chains and level playing field

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.

From the users' point of view, a trusted supply chain is fundamental to assure business and service resilience. This is particularly true for the major companies involved in critical infrastructure and services as well as those delivering major assets to the European economy and society. **Users are dependent on their suppliers and only a trusted supply chain can reduce risks of incidents** (e.g. major ransomware attacks). Today, suppliers' victims of an attack refuse to communicate such information to customers / end-operators (especially in the early stages when the ability to react decreases hour by hour). A mandatory notification process could be envisaged in the future to limit negative impacts of this dependence.

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 an open dialogue, cooperation and exchange with like-minded** (sharing same values) **international** (non-EU) **stakeholders** on cyber threats and trusted solutions (including an adequate diversification of strategic suppliers to avid dependencies) to effectively address cybercrime, in a fair and democratic governance, under **reciprocity rules.**

We should also **build a level playing field** throughout the Digital Single Market and contribute to the work **addressing the distortive effects of foreign subsidies**.

10. Develop the Next Generation Public Private Cooperation strengthening the European Cybersecurity Community to support the implement of these recommendations: ECSO 2.0

ECSO has been delivering **policy support** and **concrete actions** to improve the **European Cybersecurity Ecosystem for almost 4 years**. Today, **we have reached tangible results and brought together an EU Community of public and private stakeholders**, working hand in hand to prepare the next common steps, also in close cooperation with the E. Commission and the other E. Institutions.

These positive achievements are the result of a strengthened, innovative and efficient dialogue and cooperation gathering all categories of stakeholders across all sectors based upon an effective multiscale approach including local, regional, national and European levels of cooperation. This **unique public – private cooperation is a key element which should be continued** and upon which the future European Institutional and operational framework (c.f. the European approach on Competence Centres) should be built.

Only in an efficient public-private cooperation can we successfully face global cyber threats, increase our strategic autonomy and bring innovation for effective market implementation and use.

The building of an interlinked European and National Public-Private governance can therefore **benefit from the experience of ECSO to develop competences and common trust**. **ECSO members are fully committed to moving forward together** in this direction remaining a strong ally at local/regional, national and European level, provided that the openness, collaborative spirit and results-driven approach of the organisation are preserved.

In light of the proposal to establish a European Competence Centre, National Coordination Centres and a Community, and in order to better serve the goals and address the challenges set by these institutions, ECSO will likely have to evolve its structure (both membership and governance).

ECSO, or its possible evolution (ECSO 2.0), **should be one of the cornerstones for the construction of the future European governance in cybersecurity gathering the needed communities and experts** (in particular linking at European level the stakeholders from the national communities).

It is time to consolidate existing efforts and further structure the cooperation between national public administrations, EU institutions and the private sector, including the 4 Pilots on Competence Centres. **ECSO, with the Pilots, is already representing the European Cybersecurity Community** at regional, national and European level and is ready to build upon this in the future governance.

We are confident in the willingness of all stakeholders to further improve this excellent initiative and have **ECSO continue to be the leader of an inclusive and unified European stakeholder ecosystem in a Next Generation of Public Private Cooperation**.

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU