ECSO recommendations on cybersecurity in light of the COVID-19 crisis

Summary

In this document, ECSO reviews its recommendations to the European Commission and Parliament for a Cyber Resilient Europe (January 2020) in light of the COVID-19 outbreak and calls for recovery and stabilisation measures to be taken at European level to face the immediate, mid and long-term consequences of the COVID-19 crisis on the cybersecurity sector, as well as its economic and social ramifications in all other sectors.

As we are rapidly becoming increasingly dependent on digital solutions and services, important measures proposed in this document are tailored to address the immediate needs of the different critical infrastructure operators and industries to ensure a secure and safe continuity of their services, as well as citizens to prepare and support them in navigating the online world.

The measures proposed by ECSO are categorised according to financial, competence & awareness, investment and implementation measures that should be conducted in a collaborative approach between the public and private sector to strengthen strategic autonomy in critical sectors.

Long term post-crisis stabilisation measures are also suggested in the form of legislative proposals and broader initiatives on training, education and SME support matching the ongoing work and projects launched by ECSO. These measures are designed to address structural issues inherent to the European cybersecurity ecosystem and to ensure the recovery of sovereignty across Europe.

Finally, ECSO proposes the establishment of several funds and investments at each stage of the crisis and post-crisis timeline (emergency fund, strategic autonomy fund, R&I to market fund, fund of funds and recovery fund) to overcome the current challenges and help build a strong and competitive European cybersecurity ecosystem.

As said, these recommendations on cybersecurity in light of the COVID-19 crisis build upon and update the recommendations to the new Commission approved by ECSO earlier this year, namely:

- Creation of a vision for a European Cybersecurity and a comprehensive European Cybersecurity Industrial Policy which would essentially attract the interest of EU industry and incite the growth of European stakeholders.
- Development of an efficient public and private co-investment mechanism (and cooperation) to boost development, competitiveness and business.
- Recovery of a higher level of sovereignty (/data sovereignty) and support to the socio / economic development through an increased digital autonomy in Europe in an enhanced public – private cooperation.

State of play

Governments across Europe are intensifying their efforts to combat the global spread of the COVID-19 virus with various measures to support public health systems, safeguard the economy and ensure public order and safety.

At the same time, the coronavirus (COVID-19) outbreak has created an even more fertile ground for cyber-crime, threatening the safety of citizens and businesses in a challenging operational and financial environment. As businesses and citizens increasingly rely on digital solutions, the nature of the threat is also changing, with cybercriminals exploiting fear, uncertainty and unprecedented situations. For organised crime, cybercrime represents an alternative to physical crime as it can easily be conducted during a lockdown.

This crisis is a reminder of how crucial our digital ecosystem is to our economy, citizens, and political life. It is the invisible yet crucial foundation of today's world, upon which we rely to communicate. But this outbreak has also showed us how important is to ensure protection and resiliency of the digital ecosystem through the entire value chain.

In these challenging times, cybersecurity must be considered as an essential instrument to ensure the secure and coordinated implementation of global financial, political and sanitary contingency plans, as well as of the safety of citizens.

The move to online living is creating a number of challenges:

- Increased Internet traffic;
- Increased reliance on secure remote access technologies (including VPN – Virtual Private Networks) which employees are not always familiar with and with potentially sensitive links between professional and personal computers and associated devices (e.g., personal printers);
- Increased use of smartphones (including access to secure mobile applications) for remote conferences, exchange of documents etc.;
- Increased attack surface as more individuals work from home and part of the internal company network could be reachable from outside;
- Attacks linked to account take over, fraud, ransomware, denial of service, phishing, also targeting health systems which are particularly critical in this period;
- Increased disruption of critical suppliers (outsourced security operation centres, IT architecture management teams, etc);
- Fake social media profiles / users are spreading disinformation during periods of increased reliance on social media for critical information updates;
- Increased emergency challenges to CISOs (Chief Information Security Officers) with increased need for adequate tools for crisis management.

To be noted that certain critical digital infrastructure such as telecommunications networks have remained resilient and have coped well with the above-mentioned challenges, not resulting in major incidents or service disruptions.

We should therefore consider the following future cyber-related implications of the COVID-19 crisis:

- IT and cybersecurity, despite remaining operational during the COVID-19 crisis, could be seen as a secondary priority compared to other economic emergencies and could therefore face budget cuts to facilitate the recovery of major economic sectors paralysed by the crisis (transport, tourism, large part of industrial manufacturing, etc.);
- Users could be lured into using non-validated / non-certified low cost solutions (likely not providing an adequate and assessed level of security and trust) due to financial issues as well as product availability.

We should not forget that cybersecurity is and will be a support to economy recovery with its strong market growth. It is thus essential to urgently address ways to improve the resilience of digital processes, supply chains and critical infrastructures at local / regional, national and European level in the short and medium / long term.

In the post crisis period, we there will be an increased use of IT solutions among other to speed up the recovery of manufacturing. To facilitate the recovery from this crisis notably in the EU, we could expect accelerated digitalisation (than anticipated in the pre-COVID era) in Industry 4.0 of IoT, Artificial Intelligence, 5G, Cloud & Edge computing, blockchain, high performance computing, automatic decision making and management of large amount of data …

Cybersecurity is the “glue” linking all these technologies and their use in the different applications / verticals. The use of new technologies will help address specific needs but it will also further increase the attack surface: applications should be adequately protected against evolving threats by the “cybersecurity glue”.

This crisis has shown the need for an increased autonomy in critical / vital sectors and the recovery of a digital sovereignty. Long term sovereignty and resilience of the EU and its Member States should be recovered in the cybersecurity sector: cyber sovereignty should be one of the main driving objectives for future investments. The cybersecurity industry must be recognised as a vital sector for Europe and its countries. It could be part of those “critical infrastructures” that need to be developed, supported and preserved.

Measures suggested by ECSO

1. "Urgent measures" (by 2020): financial, skills, education & awareness, knowledge of suitable cybersecurity services (as part of the "recovery measures")

For critical infrastructure operators and professionals

- Reinforce measures to ensure that operators of essential services can maintain and make their IT infrastructure resilient and dependable in times of high demand and crisis, supported by skilled manpower;
- Leveraging upon lessons learned during the crisis, ensure the definition and implementation of best practices and cybersecurity guidelines in a cooperation between Public and Private stakeholders to cope with large scale incidents that could occur during the crisis (but experience and guidelines could remain valid also in "normal times") focussing on real time and day to day operations, limiting the physical operability of critical infrastructure and provided services.

For EU suppliers (in particular SMEs and start-ups) of cybersecurity solutions

- Support access to liquidity and credit facilities (particularly important for SMEs) to maintain their business as well as fiscal relief. Use of state aid measures should also be considered for strategic areas;
- Ensure visibility of European cybersecurity companies' offers, including SMEs, for starting and supporting the use of EU solutions (ongoing ECSO action at EU level: Cybersecurity market radar and marketing label with the support of national partners);
- Ensure implementation and use of digital applications to allow a progressive and safe exit from the lockdown, all while respecting the privacy of citizens as well as security and cybersecurity concerns, in line with the provisions of the EU toolbox for the use of mobile applications for contact tracing and warning in response to the coronavirus pandemic, published last 16th April.

For Users and Citizens / Students

- EU suppliers invited to provide free access to a number of secure services to counter cyber threats in the crisis and early post-crisis period (ongoing ECSO action at EU level: COVID-19 solidarity campaign, with the support of members and partners);
- Provide free online classes to better equip citizens / students remaining at home with the skills to navigate "online life" and protect themselves from cybercriminals (i.e. basic coding, password protection/two factor authentication, online banking, social engineering, attack/threat vectors, etc.).

For Citizens

- Run awareness campaigns on the potential risks derived from social media and online purchasing;
- Run education campaigns on cybersecurity and opportunities for a future career in this domain, also taking advantage of remote learning during the lockdown (ECSO action of Youth4Cyber started during the COVID crisis).

2. "Recovery measures" (2020 – 2021): cooperation and solidarity

Financial / Investments

- Support business continuity and economic revitalisation at EU level also by cybersecurity using EU financial instruments: European Investment Bank (EIB) guarantee schemes, specific common debt instruments, stronger synergies between public-private investments, etc.;
- Approve the next European MFF (Multi-Annual Financial Framework) without cuts expected before the crisis under the cybersecurity headings and related programmes. Review / reallocation of priorities in the MFF according to new post-crisis scenarios (including concentration of funds to main priorities and dedicated "emergency relief" budget lines with fast-track funding) should indeed take into account that cybersecurity and its multiple aspects are main priorities in a comprehensive EU "vision" to guarantee a fast and secure economic recovery;

- Increase investments on commonly redefined and agreed priorities for sensitive / strategic applications and critical infrastructures through "close to market" projects with high TRL (Technology Readiness Level), supported by procurement policies (including – where relevant - state aids: c.f. IPCEI);
- Ensure an increased strategic autonomy of the EU through:
    - A comprehensive European cybersecurity industrial policy (including the relocation of European industrial activities which have an impact on the security & safety of citizens and of the economy);
    - A dedicated fund creating synergies between public and private money for increased strategic autonomy in strategic ICT areas, including cybersecurity;
    - A wide Public - Private cooperation of European cybersecurity stakeholders: Cybersecurity is a market composed by many different technologies applied to many different applications: a specific approach would be needed in closer cooperation with the private sector for market aspects and stronger synergies for public – private investments and procurements;
- Develop specific measures to support trusted supply chains for ICT networks and applications in particular through financial support, certification and diversified trusted suppliers to increase the EU digital autonomy;
- Ensure effective implementation of the FDI (Foreign Direct Investment) screening regulation to avoid foreign acquisitions affecting strategic European programmes and strategic assets (including innovative SMEs, fragilized during and after the crisis), and also to secure a level playing field.
- Consider the possibility to make mandatory the principle of "Most Economically Advantageous Tenders" (MEAT) for strategic digital security procurements. Procurement should not only be driven by the lowest price, but the greatest value they have to societies: climate friendly, workers' rights, environment protection, job creation and life-cycle approach.

Competence & Awareness

- Facilitate the exchange of information on threats, incident reporting, and mitigation plans among operators and across the EU, particularly important in periods of crisis;
- Analyse the COVID-19 crisis evaluating also weaknesses revealed, issues and impact on the ICT sector and cybersecurity through a high level Commission - Member States - Industry return on experience, to inform the Community, publishing results for improvement of best practices and take informed decisions for future priorities & investments.

Cooperation and Investment

- Strengthen Public-Private cooperation for the EU cybersecurity ecosystem development leveraging upon the support of ECSO and the 4 Competence Centre Pilots (looking at the future European Cybersecurity Centre, national coordination centres and ECSO 2.0 to gather and have cooperating the public – private EU Cybersecurity Community) to re-define priorities for R&I (Horizon Europe) and DEP (or other EU funds) in the light of the post-COVID society and market evolutions;
- Establish a comprehensive plan for Public – Private investments from R&I to market (basic and applied research, capability development, infrastructure capacity building, operational capacity building / short term needs for economy, society and national security);
- Establish a fund of funds specific to cybersecurity (cybersecurity needs a specific approach, being different from other ICT domains) to boost investment / procurement and economic recovery in Europe (technologies, components, products, services, SMEs … Ongoing ECSO effort in this direction with the support of main investors across Europe).

Development and Implementation

- Support development and implementation of European solutions for an increased strategic autonomy in security architectures and security operations: key technologies (AI, blockchain, IoT …), infrastructure (Internet, Cloud / Edge, 5G …) and services (European SaaS - Security as a Service offer with MssP - Management of security services Providers - EU champions, SaaS-delivered network connectivity, Software

defined network architectures and security; Virtual SOCs - Security Operation Centers enabling remote analyst work in compliance with EU privacy and data protection rules, SASE - Secure Access Service Edge);

- Ensure financial support to develop secure cloud services and data centres in Europe to better control data flow and secure data management in times of crisis (and beyond), particularly in the healthcare sector (also as envisaged by the EC in its recent EU data strategy communication);
- Establish process guidelines for a comprehensive approach in vulnerability management for crisis readiness. This approach would consider use of tools for threat identification, continuous security assessment and certification compatibility;
- Support the development and implementation of a strategy on cyber threat intelligence as well as on the exploitation and processing of data to ensure European sovereignty. Leveraging upon common technical elements for data exchange it would be the basis of a collective European cyber threat knowledge effort to protect the re-launching of the economy, of critical infrastructures, data, etc.;
- Support the better management of virtual IDs (for trusted exchanges) and the use of Data Loss Prevention by EU service providers to ensure that sensitive data is not lost, misused, or accessed by unauthorised users and enhance or extend crisis situations;

3. "Stabilisation measures" (from 2021)

Legislations

- Consider the activity of CISOs (liability issues) and digital risk management considerations in future legislation to reduce cyber vulnerabilities and help them allow their Boards of Directors to take suitable informed decisions, in particular when re-evaluating priorities for spending plans and better mitigation of crisis situations;
- Incentivise the use of future EU certified products & services, which is certain cases could be made mandatory also to support increased strategic cyber autonomy;
- Consider and incentivise in EU legislations purchasing preference of European solutions (EU integrators) and services, when available and appropriate, for sensitive data & applications;

Capacity building, training and jobs

- Support the use of cyber ranges for simulation-based crisis management, training of staff, and simulation of attacks. Consolidate existing efforts in Europe on federating cyber ranges and build a "cyber-range-as-a-service" platform to serve the Community and be better prepared in case of crisis (a one stop shop to build, acquire, or complement cyber ranges for commercial, education/training, R&D, Critical Infrastructures or national security/military use). Sector-specific ranges could be used to better inform policy making and users' needs;
- Support cybersecurity training and professional development, also through European professional profiles;
- Establish a European cybersecurity job platform using interactive tools and simulation of career pathways with link to verification of skills. The tool should be a resource for employers (facilitate hiring), educators (adapt curricula to fit needs), job seekers (one stop shop for job search), students (understand possible career pathways), and policy makers (develop policies to fit the needs of the job market and support the growth of the economy).

Support to SMEs and regions

- Support the creation of European accelerators for SMEs, in cooperation with local / regional / national stakeholders to build ecosystems of trust at all level;
- Support the implementation of ICT and cybersecurity at local level supported by specific financial measures to help the recovery of local / regional economies.