L.REBUFFI speech at ITU on September 17th

Good afternoon ladies & gentlemen. Thank you to ITU for the kind invitation – I'm very pleased to be with you today even if I would have preferred the traditional way of meeting in person.

These are strange times but I think that they have also forced us to re-shape our thinking, not just in the way we work but also in what we can do - to better protect our society & economy.

Indeed, across Europe, intensive efforts have been made to combat the global spread and effects of the coronavirus pandemic with various measures to support public health systems, safeguard the economy and ensure public order and safety.

At the same time, the outbreak has created an even more fertile ground for cybercrime, 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.

To explore the effects of the COVID-19 crisis, from March to May 2020, ECSO conducted surveys internally with members as well as externally with the community, in order to better understand the impact of the pandemic on the activity of cybersecurity stakeholders during the crisis period, as well as their expected challenges post-crisis.

Respondents came from all categories of cybersecurity stakeholders in Europe: RTO's/universities, regions, SME's, Large Companies (users and providers), public administrations, EU institutions/agencies, users/operators and associations.

We were able to obtain 5 key takeaways from the results of those surveys:

- During the pandemic, an increase in cyberattacks and cybercrime (in particular fraud and malwares) has been the top concern for organisations.
- One of the main concerns for organisations post-crisis is that they have a lack of understanding of how the market has changed and will evolve (for their organisation's business, activity, etc).
- When we look at critical infrastructures, the most significant increase in cyber attacks has been experienced by the healthcare and financial sectors during the crisis. Also, public services, e-government, and digital citizenship sector were indicated as relevant sectors to have suffered a strong increase of cyber threats together with remote working challenges that citizens have faced with the sudden and complete shift to online working.
- The cybersecurity community believes that stronger public funding for research and innovation and a shorter cycle from research to market as well as investments to protect data and vital services with respect to potential new disruptive challenges are fundamental aspects needed to recover activities after the COVID-19 crisis.
    - In particular, Artificial Intelligence, 5G & future communications networks, IoT and cloud / edge computing are the key technological areas which will have a drastic impact on the future.
    - Also, infrastructure resilience and data (including privacy) are particularly pertinent priorities to be tackled by the future Commission funding programmes.
- The results from our survey, but also in the different webinars we are following these days, showed that the community expects a higher public-private cooperation, with an approach similar to what developed by ECSO, to boost advocacy, awareness, cyber resilience measures, visibility for solutions, investments, capacity-building & competitiveness.

  One of the main areas in the PPP includes also an increased cooperation on threat intelligence between public CERTs and private operators which are at the forefront of cyber threats and attacks. A strong & resilient cybersecurity ecosystem in Europe is simply not possible without the active engagement of the private sector. The ongoing discussion on the review of the NIS Directive could be an opportunity to better take into consideration effective operational aspects from providers of vital services and operators. To improve the dialogue, at least on the private side, in ECSO we have developed a specific Users' Committee to boost the strategic cooperation across CISOs of different countries and sectors.

In light of these results, we identified a set of recommendations aimed at guiding public-private efforts to manage and recover from the effects of the pandemic and boost the cybersecurity resilience of our society, economy and infrastructures.

We have an opportunity to make Europe a leader in cybersecurity but we need proper funding, investment, and access to market to achieve this. The recommendations are therefore geared towards steering investments, public-private cooperation, and technologies in cybersecurity in Europe in the years to come, and could present them across 4 pillars.

First, we must invest in Europe & foster strategic partnerships

This includes:

- Increasing investments on commonly redefined and agreed priorities for sensitive / strategic applications and critical infrastructures through "close to market" projects.
- Reinforcing 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. A stronger strategic and operational cooperation between these operators and the public sector for a better threat intelligence, prevention and response should also be envisaged .
- Supporting the accelerated digitalisation in Industry 4.0 of IoT, Artificial Intelligence, 5G, cloud & edge computing, blockchain, high performance computing, automated decision making and management of large amounts of data.
- Investing in cybersecurity on a massive scale (e.g. venture capital, public-private co-investment) as it represents the "glue" linking all technologies and their use in the different applications / verticals.

Secondly, we should leverage European assets & increase R&I funding

When looking at the future R&I landscape, efforts should be made to:

- Re-define priorities and increase funding for European R&I in light of the post-COVID society and market evolutions.
- Ensure that research funding covers the full spectrum of the cybersecurity industrial ecosystem, from infrastructure resilience, data & privacy, and risk management, but also skills to support EU competitiveness.
- Leverage on Europe's strongest assets and showcase European cybersecurity champions in research, drivers of industrial innovation, and data & privacy ambassadors on a global scale.

Third, it is essential to boost European competitiveness

There are a number of ways to do this but priority must be given to:

- 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.
- Develop a specific approach to consolidate the European cybersecurity market in closer cooperation with the private sector for market aspects and stronger synergies for public-private investments and procurements.
- Engage the cybersecurity industry to support the economy recovery with its strong market growth.

Finally, we must place cybersecurity at the heart of Europe's digital sovereignty and strategic autonomy

For this we must:

- Make cyber sovereignty one of the main driving objectives for future investments in Europe to ensure that our future is digital and secure.
- Increasing autonomy in critical / vital sectors and recover sovereignty and resilience of the EU and its Member States.

- Differentiate, and validate through certification, external supply sources in areas where Europe cannot develop its own products.
- Recognise the European cybersecurity industry as a vital sector for the Union and its countries, and make it part of our "critical infrastructures" that need to be developed, supported and preserved.

As ECSO, we remain dedicated to continuing in a public-private cooperation to achieve these fundamental cybersecurity objectives over the coming years and we will continue in our role of federating the European cybersecurity public – private community, promoting and supporting policies and concrete actions.

As the President of the European Commission Ursula Von Der Leyen said in her State of the Union speech yesterday, the next 10 years will be "Europe's Digital Decade" and as we know, cybersecurity will be and should be at the very heart of this. I look forward to working with all of you in this goal.

Thank you for your attention.