NAVIGATING CYBERSECURITY POLICY IN THE EU: A CALL FOR NEW LEGISLATORS

ATTN: CYBER AND DIGITAL POLICY ADVISERS

In the digital and cyber domain, today EU countries face serious external threats regardless of some of the differences that traditionally shield them from the risk of conflict, such as geography, political leanings, and economic standing. They also face internal challenges to effectively manage the cybersecurity ecosystem setup for defence and resilience.

To advance the level of cybersecurity maturity across the Union and in each Member State, it is fundamental to rely on ***strong bipartisan political will****, supported by* ***sectoral professional expertise****. In line with the transversal nature of cybersecurity, the legislative framework developed over the last decade advances the key political priorities of multiple different parties. Collaboration between all stakeholders is highly needed to safeguard EU citizens and countries from cyberattacks.*

For these reasons, we call on all new legislators to endorse existing cybersecurity initiatives, defend and advance European values and interests, support public-private cooperation, and engage with cybersecurity professionals and experts.

External Threats and Internal Challenges

If in the physical domain, a country's location granted a degree of material protection, putting distance between a potential attacker and a defender, cyberspace instead neutralises all distances. Whether you neighbour your enemy or there is an ocean in between, distances play a much less relevant role when pursuing a cyberattack. Likewise, while a political party's foreign policy can impact international alliances, this does not necessarily shield a country from the activity cybercriminals and country-affiliated threat groups, often following opportunistic interests. Last, even intra-EU economic differences, which often dictate EU policy making, are less strongly correlated with the likelihood of being victim of a cyberattack. Most EU countries still rank as high-income societies compared to the rest of the world, making them naturally high-value targets for financially motivated attacks.

As EU countries operate in this environment, they also have to consider internal challenges. After legislating extensively, the EU now has to move into the implementation phase, ensuring the effective management of the designed cybersecurity ecosystem. Considering the number of stakeholders coming together – whether they are public or private actors, European, national, or local entities – the complexity to set up and run all the initiatives foreseen is not trivial.

Key EU Cybersecurity Policies

The cybersecurity domains touches upon a wide range of issues, from national security to economic prosperity, to citizen's rights and liberties. Notwithstanding all limitations and areas of improvements, every one of the EU policies passed over the last legislation enhances a wide spectrum of political priorities due to the deeply transversal nature of cybersecurity. Three examples worth looking into are the following:

- The **NIS2 Directive**, officially published in January 2023, aims to increase the overall level of cybersecurity in Europe in the long term, by establishing cybersecurity requirements and incident reporting obligations for entities belonging to critical sectors. On one hand, the Directive strengthens each nation's sovereign critical assets by improving their cybersecurity posture, while also letting Member States lead the implementation. On the other hand, EU citizens will be able to rely on more secure services offered by the critical sectors' entities and ultimately a higher level of protection for their data. Last, from an EU perspective, the NIS2 Directive further consolidates and harmonises the approach to cybersecurity. As a result, both national sovereignty and public welfare are strengthened.
- The **Cyber Resilience Act** (CRA) tackles cybersecurity focusing on products, instead of organisations, like the NIS2 Directive does. Given today's unbearable state of vulnerabilities impacting software and hardware products, the CRA Regulation attempts to improve product security by defining baselines for manufacturers. This leads to enhanced consumer protection, as all users of commercial products produced or sold in the EU can expect more secure products, since vendors are required to implement security measures and address known vulnerabilities. This represents a significant step forward to the benefits of end-users. Once the workflow is established, national authorities will also gain a more accurate overview of vulnerabilities being actively exploited, in synchronisation with ENISA, allowing them to issue advisories and respond to active incidents. The overall security of the digital supply chain in the EU and beyond will benefit from these improvements.
- The **Cyber Solidarity Act** (CSoA) aims to set up three innovative initiatives in Europe: a pan-European information sharing system, a Cyber Reserve consisting of trusted cybersecurity providers capable of augmenting the capacity to respond to incidents around Europe, and finally a mechanism to investigate the root causes of critical incidents and draw lessons learned for the future. The CSoA promotes key national cybersecurity companies, providing them additional business opportunities through the Cyber Reserves, while fostering EU incident response capabilities. It also promotes cooperation among EU and other European national stakeholders, through the setup of platforms, networks, and cooperation arrangements to exchange information about threats and incidents.

The NIS2 Directive, the CRA, and the CSoA represent three examples of EU policies developed over the last legislative, which benefit national interests, citizens, and the EU as a whole. They are not perfect – there will be opportunities to improve them in the future – yet they strike a fair balance between political priorities pursued by different parties' agenda.

The Case for Bipartisan Support in Cybersecurity

As an inherently transversal field, in a democracy, cybersecurity requires that diverging goals and perspectives come together. Promoting economic growth and market initiative without any constraints puts fundamental rights and liberties at risk, whereas overly extensive protections hinder a dynamic market capable of developing strong security solutions. Maximising national security, for example by granting encryption backdoors to law enforcement, creates vulnerabilities that can be exploited by malicious actors as well. Resources allocation follows a similar approach. Security will always require a balance between rights and liberties and economic drivers. Cybersecurity can be achieved only through a carefully calibrated balance between different priorities, which fundamentally lies on bipartisan actions.

Cybersecurity is too critical to be sidelined or become polarised. While important steps have been achieved so far, ensuring effectiveness and efficiency is the main challenge in the upcoming years. ECSO is ready and willing to discuss with any interested MEPs the topics at hand, provide an overview of the different policy positions and their contentious points under debate, as well as the different political perspectives and the available evidence supporting them. For these reasons, we call on all new legislators to:

1. **Endorse existing cybersecurity initiatives**: After designing an articulated legislative framework, advancing cybersecurity in Europe requires political support both at the national and European level for a swift and effective implementation. This political support should be bipartisan, building on collaboration between different political and institutional stakeholders.
2. **Defend and advance European values and interests:** European countries and citizens will be more secure when the protection of European values is balanced with a thriving European industry.
3. **Support private-public cooperation**: Considering the fine balance between private enterprises and public administrations in the cybersecurity sector, cooperation and partnerships should be further developed.
4. **Engage with cybersecurity professionals and experts**: Due to the multi-disciplinarity of cybersecurity, policies and initiatives should be grounded in empirical evidence and data-driven insights, engaging professionals and experts from different sectors.

Axel

Axel DEININGER	Luigi REBUFFI
ECSO Chairman of the Board	ECSO Secretary General and Founder