24 APRIL 2025

The imperative of global harmonisation of cybersecurity rules for collective defence

Executive summary

The annual cost of cybercrime worldwide is projected to hit €14 trillion by 2029, turning it into the world's third-largest economy.[1] Threat actors are using new tactics and technologies to target individuals, businesses of all sectors and sizes, governments and NGOs. They are taking learnings from one part of the world to attack another. In a world where we are all targets of common cyber adversaries that operate across borders, collaboration is key and harmonised approaches to cybersecurity policies will determine our ability to fight cybercriminals.

The EU's role in the harmonisation of cybersecurity rules globally is crucial. The EU must continue to champion an open global ecosystem and harmonised approach. To become a digital powerhouse in the domain of cybersecurity,[2] policy makers must prioritise the following:

- Pursue **international cooperation** through existing multilateral structures, starting from the G7;
- Aim for **harmonised regulations** on cybersecurity;
- Promote development and adoption of **global standards**;
- Strengthen and expand **mutual recognition agreements**;
- Enable **cross-border data flows**; and
- Promote **public-private partnerships**.

[1] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[2] See *Europe 2030: A Digital Powerhouse. DIGITALEUROPE's manifesto for the next Commission*, available at https://cdn.digitaleurope.org/uploads/2024/04/DIGITAL-EUROPE-MANIFESTO-2024-FULL-FINAL-2024-UPDATE.pdf.

Table of contents

International cooperation

Multilateral and international cooperation

Given the global nature of cyber threats, it is essential to ensure convergence to effectively bolster defences and prevention. Multilateral fora such as the G7 should foster policies that advance interoperable, flexible and proportionate approaches to cybersecurity. G7 countries should increase cooperation – in line with existing international frameworks – on cyber threat information sharing, securing networks, cloud services and digital infrastructure. This is why every year, tech associations from all G7 countries come together in the Tech7 to advance collaboration.[3]

Other organisations, such as the OECD and OSCE through their work on confidence-building measures for cyberspace, should be leveraged for political commitments from senior government leaders to fight cybercrime together.[4] These political commitments should come with a list of concrete actions or pledges, and governments should work with the private sector, civil society and academia to meet them. To track progress, the OECD should convene at multistakeholder cybersecurity summits on an annual or bi-annual basis.

At the same time, efforts in the United Nations to raise awareness across states should be maintained. The United Nations has an important role to play in capacity building and digital inclusion of those who do not have the financial capacity to protect themselves, such as developing countries or NGOs. through initiatives such as the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace.[5]

Bilateral cooperation

Bilateral cooperation plays an increasingly important role in addressing global threats. The EU has established Cybersecurity Dialogues with several important partners including the US, UK and Japan. Bilateral cooperation needs to not only be maintained but significantly strengthened in the coming years.

ENISA should play an active and strong role encouraging this cooperation, doubling down on ongoing efforts with third-country cybersecurity agencies to develop a cohesive response to cyber threats that transcends national borders.

[3] https://www.digitaleurope.org/news/tech-7-joint-declaration/.

[4] https://www.osce.org/files/f/documents/f/7/555999_1.pdf.

[5] https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

Concurrently, several jurisdictions are updating their cybersecurity rules, such as the UK's preparation of its own Cyber Security and Resilience Bill.[6] ENISA should engage with these jurisdictions, with the aim of leveraging existing approaches and, where possible, harmonising these frameworks to minimise lift, and ensuring cohesion with new legal obligations.

Regulatory harmonisation

A harmonised regulatory cybersecurity framework is crucial to ensuring cybersecurity resilience and maintaining the EU's global competitiveness. Pursuing common, consistent and proportionate regulation minimises unnecessary fragmentation and creates a predictable environment for businesses.

Divergent regulations can lead to inefficiencies and friction, particularly when dealing with regulators in multiple different states. This has the effect of forcing organisations to prioritise regulatory compliance, sometimes at the expense of best practices. Fragmentation also increases the burden on government resources, diverting attention and limited cybersecurity expertise away from core security priorities towards regulatory compliance. Effective regulation requires a collaborative effort between public and private sectors to achieve desired policy outcomes. By working together, these forces can avoid creating further barriers and ensure more comprehensive and effective solutions. Regulatory coherence will facilitate secure digital supply chains, promote trust in digital infrastructure and drive technological innovation.

Standardisation

To create global economies of scale and enhance competitiveness, globally recognised, industry-driven standards on cybersecurity, including on incident reporting, should be the basis of any rules. Through active participation in the international standards-setting bodies and processes, the EU can leverage global expertise, promote European standards internationally and reduce compliance costs for European companies. We need to reaffirm and promote international standards to ensure the outcome is recognised as globally relevant best practice, whilst also driving investment in skills development and knowledge transfer across borders.

Transposing existing international standards for emerging purposes is paramount. At the same time, the EU is currently developing standards for products with digital elements, in the context of the Cyber Resilience Act (CRA).[7] Such efforts should stay closely aligned with other ongoing efforts in other jurisdictions to avoid duplication of work or diverging standards. Existing standard at international level should be used as much as possible in order to

[6] https://www.gov.uk/government/collections/cyber-security-and-resilience-bill.

[7] Regulation (EU) 2024/2847.

facilitate the presumption of conformity with the essential requirements of the CRA. The objective of standards should remain to facilitate the free movement of goods and services in the single market.

Intergovernmental mutual recognition agreements

Intergovernmental mutual recognition agreements (MRAs) are essential for facilitating market access, ensuring non-EU products meet high standards and preventing regulatory fragmentation. These agreements allow for non-EU countries to facilitate conformity assessments by accepting the designation of conformity assessment bodies outside of the EU and vice versa. However, current MRAs with key partners such as the US and Japan cover only a limited range of products, and discussions on cyber are in most cases in very early stages and only slowly moving forward. Given the growing role of New Legislative Framework legislation in the EU and the increasing prevalence of global cybersecurity requirements, expanding these agreements to cover digital products should be a priority.

Enable cross-border data flows

Ensuring the free flow of data across borders is vital to combat cybercrime around the world. As cybercriminals are increasingly establishing sophisticated global networks, restrictions on data flows can hinder business innovation, disrupt supply chains and complicate our ability to combat cybercrime. Today, an attack can take place in Brazil, threat actors move to Indonesia and then the attack happens again in Germany.

Security is often cited as a justification for data localisation, but on-soil storage alone does not enhance nor guarantee protection. Building secure and resilient systems requires seamless data transfers to detect threats in real time, ensure business continuity and allow for effective responses to cyber incidents. Possessing the ability to collect and holistically analyse data, identify threat trends, and share those insights across borders and with multiple stakeholders is essential in our shared fight against cyber criminality.

Data localisation frameworks can lead to serious unintended consequences on both domestic and international stakeholders, raising the cost of digital services, particularly for SMEs, increasing vulnerability to cyber-crime and fraud, and creating barriers to both the adoption of innovative technologies and the broader facilitation of digital trade. Requirements to store locally or prevent data from being processed overseas, as a condition for doing business in a country, can undermine cybersecurity efforts in the following ways:

- **Fragmented view of the threat landscape puts consumers at risk:** Localisation limits our ability to spot global threat trends and hinders our overall ability to share and collect cyber threat intelligence globally.

- **Increased virtual and physical access points:** Local storage requirements result in more physical locations to secure – increasing overall security risk.
- **Reduced efficiency and resilience:** Localisation requires the use of outsourced services, leading to reduced efficiency, added costs and less resilient delivery of services.

Public-private partnership

Cybersecurity threats are inherently agnostic to geographical borders and sectoral distinctions, necessitating a comprehensive strategy that bridges the divide between public and private entities. Given that a substantial portion of critical infrastructure is operated by private sector organisations worldwide, a holistic approach is imperative. This entails recognising cyber resilience as an interconnected entity, rather than isolating individual components such as financial institutions, ICT systems or connected devices.

To achieve this, it is essential for private organisations and regulatory bodies to collaborate in identifying and addressing vulnerabilities within the supply chain. Public-private partnerships allow for:

- A regulatory framework that takes into account how rapidly technology evolves, along with the related threats.
- A holistic view of cyber resilience, given the cross-sector and cross-regional nature of cybersecurity.

Global fora such as the G7, G20, UN, WTO, APEC and OECD and other multilateral organisations, should ensure a multi-stakeholder approach and enhance public-private dialogue. International sectorial ISACs is one model of public-private partnership that could be further enhanced.

In the same vein, bilateral dialogues are essential to coordinate cyber initiatives and engage the private and public sectors. The EU-US Cyber Dialogue delivered important results and should be continued. As DIGITALEUROPE, we are ready to contribute to its development, as we have done over the past years.

FOR MORE INFORMATION, PLEASE CONTACT:

Rita Jonušaitė

Senior Manager for Cyber & Cloud

rita.jonusaite@digitaleurope.org / +32 499 70 86 25

Sid Hollman

Policy Manager for Cybersecurity, Infrastructure & Mobility

sid.hollman@digitaleurope.org / +32 485 55 22 54

DIGITALEUROPE

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.