Norwegian Institute
of International
Affairs

POLICY BRIEF – 8 / 2024

Digital Borders, Global Ties: The EU's Dual Quest for Cybersecurity and Digital Sovereignty

Claudia Emilie Aanonsen

Summary

- EU visions toward 'digital sovereignty' and cybersecurity respond to concerns over geopolitical instability, data ownership, and control over digital infrastructures and critical assets.
- The EU faces challenges in balancing digital sovereignty (control over its digital ecosystem) with international cooperation including NATO and the U.S. market.
- EU regulations strive to reduce global interdependencies but risk isolation from global competitive markets and integrity of data flows. EU and EEA members must tackle demands of global integration with EU visions of digital sovereignty.

The Ukraine war has catalysed changes in European Union (EU) cybersecurity policies. Russia's offensive cyber capabilities and Ukraine's resilience to such attacks have captured the attention of the EU, placing emphasis on the importance of strengthening its cybersecurity framework. This shift is also driven by growing concerns over European data ownership, national control over digital infrastructures, and the protection of critical assets from external threats. At the intersection of security and economic interests, the EU faces the challenge of balancing its ambitions to achieve 'digital sovereignty' - ensuring control over its digital ecosystem - with wider economic goals and security concerns. This policy brief explores how the EU's evolving cybersecurity landscape is organized through regulatory frameworks that aim to underpin the EU's security strategy and bolster its role as a cybersecurity actor on the global stage.

A central part of this effort is the forthcoming *Cyber Resilience Act* (CRA), which aims to establish stricter cybersecurity standards for digital products and services in the EU. The CRA is emblematic of the EU's broader vision of digital sovereignty, which seeks to fortify geographical borders and ownership and strengthen the digital single market. However, this vision conflicts with the EU's reliance on international connectivity and cooperation, particularly in cybersecurity, where relationships with external actors (such as NATO and U.S.-based tech companies) remain crucial for the integrity of information flows and digital products and services. This tension between territorial digital sovereignty and jurisdictional cooperation presents a significant challenge for the EU as it navigates its dual quest of securing its digital infrastructure and maintaining global alliances. The CRA reflects the EU's struggle to reconcile competing notions of sovereignty and its ambitions to be a more autonomous cybersecurity actor, while also addressing implications and opportunities for the digital single market.

EU cybersecurity ambitions

Historical context

The EU has increasingly recognized cybersecurity as strategically important, positioning itself as a key player in the global digital security landscape. This shift has been driven by the growing realization that digital security is fundamental to economic stability, national defence, and the protection of citizens' rights. The intensification of cyber threats, particularly in the wake of geopolitical and European crises like the Ukraine war, has accelerated the EU's motivation to aim for a more coordinated, unified approach to cybersecurity. In the lead-up to Russia's invasion of Ukraine in 2022, for example, the Ukrainian government enacted a pivotal law allowing the migration of critical public and private sector data to abroad data servers. This decision, supported by U.S. companies like Microsoft and Amazon, was driven by concerns over the destruction of local data storage systems. While this move safeguarded essential data, it also exposed vulnerabilities related to data ownership and privacy, raising questions about the growing reliance on foreign cloud providers – also for the EU.

Aiming to ensure greater control over its digital infrastructure, data regulation and governance, the EU is pursuing digital sovereignty. *The EU Cybersecurity Strategy for the Digital Decade* (2020) outlines a comprehensive framework to strengthen the digital resilience of member states, emphasizing both the protection of critical infrastructure and the need for cooperation between public and private sectors. This strategy aligns with other EU initiatives, such as *Shaping Europe's Digital Future* and the *Recovery Plan for Europe*, that seek to create a secure, resilient, and competitive digital ecosystem. The EU's emphasis on cybersecurity is not just about mitigating apparent cyber risks, but also to assert regulatory power on the global stage. This is partly driven by the growing impression that the EU must handle external threats and foreign dominance in the digital market.

Historically, the EU has championed an open, competitive global market, but concerns over data privacy, especially following the Snowden revelations in 2013, have led to a shift in its approach to digital governance. The inception of the *General Data Protection Regulation* (GDPR) marked a significant turning point, as it redefined the EU's stance on data privacy and set new standards for international data transfers. This has had far-reaching implications for Europe, particularly in challenging the dominance of U.S. tech companies. As part of its strategy for digital sovereignty, the EU has sought to reduce its dependence on foreign technology and to establish alternatives that align with European values. This direction is shaped by the EU's response to global instability, particularly in the context of the U.S.-China trade war and Russia's growing offensive, leading to a stronger emphasis on securing critical industries and data. The EU's vision of digital sovereignty is thus twofold: it seeks to protect citizens' rights through robust data privacy protections, while also addressing the complexities of data flows and cross-border governance, which poses both challenges and opportunities to data security and integrity.

The EU as a cybersecurity actor

The EU's role as a cybersecurity actor is shaped by a range of initiatives, agencies, and regulatory frameworks. The European Cybersecurity Agency (ENISA), established in 2004, plays a central role in promoting cooperation and coordination among EU countries. ENISA supports the implementation of cybersecurity policies by providing expert advice, joint exercises, and fostering 'best practices' to improve incident preparedness. These efforts are supported by regulations that lay the legal groundwork for producing national cybersecurity capabilities and shaping a unified EU response to emerging threats:

- **General Data Protection Regulation (GDPR) (2018):** GDPR protects personal data and privacy. It mandates organizations to implement technical and organizational measures for data security and requires reporting and information sharing.
- **EU Cybersecurity Act (2019):** The Cybersecurity Act strengthens ENISA's role and establishes an EU-wide cybersecurity certification framework for ICT products and services.
- **EU Cybersecurity Strategy for the Digital Decade (2020):** The strategy outlines the EU's vision for a secure and resilient digital environment, focusing on building cybersecurity capacities, enhancing collaboration, and promoting secure technologies.
- **NIS2 Directive (2022):** NIS2 (extending the scope of the NIS Directive) asserts requirements for security standards and incident reporting for essential services, risk management, and digital service providers.
- **Digital Services Act (DSA) (2022):** The DSA addresses online platforms and digital services, including cybersecurity provisions. It requires platforms to take measures against illegal content and disinformation.
- **Cyber Resilience Act (CRA) (2024):** The CRA establishes harmonized cybersecurity rules for all digital products

and services across the EU. It mandates security requirements for a wide range of products and promotes a secure-by-design production approach.

The regulatory landscape is not organised without tensions, particularly relative to goals of digital sovereignty. While the EU aims to assert greater control over its digital infrastructure and data governance, it also faces the challenge of maintaining an open, interoperable digital market. The regulations also reveal complexities of balancing national security with economic interests. This dual approach reflects the EU's ambiguous claim to digital sovereignty, which is not only about controlling the internal digital space but also about navigating external dependencies. As the EU seeks to reduce reliance on external actors and increase autonomy in its digital space, it must navigate the risks of isolating itself from global markets, creating a delicate balance between strengthening security and fostering international cooperation. These tensions highlight the complexities of the EU's cybersecurity identity, as it grapples with the competing demands of territorial control and global integration. The next section highlights the CRA as an illustration of these tensions.

The Cyber Resilience Act

Objectives

The Cyber Resilience Act (CRA) was first announced in the 2020 EU Cybersecurity Strategy and adopted by the European Council in October 2024 (as per November 2024 it is in the process of entering into force). The CRA is a major legislative initiative aimed at harmonizing cybersecurity practices across member states. By setting stringent cybersecurity standards for digital products and services, the CRA aims to enhance the overall security posture of the EU, with an ambition to ensure that all member states are equipped to withstand and mitigate cyber risks. This move aligns with the EU's preservation of internal security: protecting its digital infrastructure, safeguarding citizen data, and reducing vulnerable interdependencies in the face of external cyber threats. The CRA can be summed up to achieve the following key objectives:

1. **Harmonization of cybersecurity standards:** One of the primary goals is to establish uniform cybersecurity certification standards for digital products and services. The EU aims to ensure that all member states adhere to high cybersecurity standards, reducing vulnerabilities across the internal market.
2. **Enable businesses and consumers to use digital products securely:** Creating conditions for users to consider cybersecurity when selecting and using digital products, ensuring they have access to clear and understandable information about a product's security features.
3. **Promotion of secure digital products:** The CRA emphasizes the importance of embedding security measures into the design and development of digital products and services. By promoting secure-by-design principles, the EU seeks to mitigate risks associated with software and hardware vulnerabilities.

Implications

What sets the CRA apart from other EU cybersecurity regulations is its significant role in advancing the EU's vision of digital sovereignty, which speaks to more than protecting digital infrastructure, safeguarding citizen data, and reducing vulnerabilities. It addresses both an economic and security concern, particularly as the EU becomes more cautious of its reliance on U.S. and other foreign tech companies for critical infrastructure and digital products and services. Although the CRA embodies increasingly restrictive legislation on data privacy whilst ensuring the protection of fundamental rights, the legislation can also be interpreted as a move toward what has been described as 'regulatory mercantilism' in the EU (see further reading for more details). Regulatory mercantilism as a form of governance responds to increased fear of external threats caused by geopolitical unrest. This comes to light as the EU seeks to reduce interdependencies beyond its geographical borders. In extension of visions of strategic autonomy, regulatory mercantilism promotes territorial control over emerging technologies through 'exporting' regulation; both as a guarantee of security, but also to rally economic advantage by promoting European standards for security-by-design for digital products and services. Through the CRA, as one of several EU regulatory initiatives, we are witnessing a reduction of global interdependencies in real time.

This bids a refocusing on the tensions that emerge from the EU's approach to digital sovereignty. Reducing foreign dependency whilst opening a space for strengthening European digital capabilities bolsters EU autonomy in the digital space. It also complicates the balance between protecting European interests and maintaining global connectivity, cooperation and competitive market. Global cooperation is a prerequisite to maintain sought-after standards in cybersecurity with regards to the flow of information, but also keeping in mind that providers of digital services and critical infrastructure to Europe remain in the hands of U.S. tech companies. Thus, the CRA should be understood as a significant but also controversial step in the EU's digital strategy.

The situation in Norway: Challenges and opportunities

As a member of the European Economic Area (EEA), Norway is closely aligned with EU policies and is a full member of the internal market. Norway adheres to many EU regulations, including NIS2 and the impending CRA (part of the EEA agreement). This relationship presents both challenges and opportunities for Norway as it navigates the cybersecurity landscape and the EU's complicated approach to digital sovereignty.

- **Integration with EU cybersecurity policies and regulations:** As Norway implements the CRA, it must ensure that national legislation aligns with EU standards. This integration can be challenging if Norway's existing frameworks differ significantly from those established by the CRA.

- **Policy influences limitations:** As a non-EU member, Norway is excluded from drafting proposals (in the European Commission) and amendments (in the European Parliament and EU Council of Ministers). Norway contributes informally but must implement the CRA as it is decided by the EU.

- **Resource limitations:** While having a robust cybersecurity framework, Norway faces resource constraints compared to larger EU member economies. Ensuring adequate funding and expertise to comply with the CRA may pose challenges for smaller organizations and businesses.

- **Collaboration and information sharing:** Norway can leverage its EEA membership to enhance collaboration with EU member states on cybersecurity initiatives. Participation in joint exercises and information-sharing platforms can bolster Norway's cybersecurity posture.

- **Innovative solutions:** Norway's strong emphasis on technology and innovation provides an opportunity to develop cutting-edge cybersecurity solutions. By investing in research and development, Norway can contribute to the broader EU cybersecurity ecosystem. The CRA provides Norwegian companies with market opportunities since Norway is a part of the internal market.

Conclusion

The tension between fostering territorial sovereignty and embracing global cooperation poses a significant challenge for the EU. While the CRA embodies the EU's ambition to bolster its digital resilience and assert autonomy, it also highlights the delicate balance the Union must strike between securing its digital borders and participating in the interconnected global digital economy. However, the drive for greater autonomy must contend with the practical realities of international interdependencies, particularly in cybersecurity, where the EU's relationships with external actors remain indispensable for maintaining current state of security for the integrity of digital information flows. As the EU navigates these complexities, the challenge remains: how to safeguard European interests and data privacy while ensuring that international partnerships continue to support the Union's broader economic and security needs. Norway in this context must balance limited influence in the EU with its relationship to NATO and dependence on the global market. Ultimately, the EU's path forward will require a nuanced approach that reconciles its rather vague aspirations for digital sovereignty with a relationship to an interconnected world.

Further reading

Adler-Nissen, R., Eggeling, K. The Discursive Struggle for Digital Sovereignty: Security, Sovereignty, Rights and the Cloud Project GAIA-X. JCMS, 62: 4 (2024) 993-1011

Bradford, A. The Brussels effect: how the European Union rules the world. Oxford University Press, 2021

Farrand, B., Carrapico, H., Turobov, A. The new geopolitics of EU cybersecurity: security, economy and sovereignty. International Affairs, 100: 6 (2024) 2379-2397

Pawlak, P. and F. Delerue, Eds. (2022). A language of power? Cyber defence in the European Union. Paris, European Union Institute for Security Studies (EUISS)

von der Leyen, U. State of the Union address by President von der Leyen, 2021; 2022; 2023

Claudia Emilie Aanonsen is a Doctoral Research Fellow at NUPI and part of the research group on Security and Defence. Her research focuses on technology, digitalisation and security. She is currently writing her PhD at the University of Amsterdam.

Photo credit: ChatGPT

NUPI Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from shortterm applied research to more long-term basic research.

NUPI
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, N-0130 Oslo, Norway
post@nupi.no | nupi.no