Key Threats to Digital Trade 2025

European Union

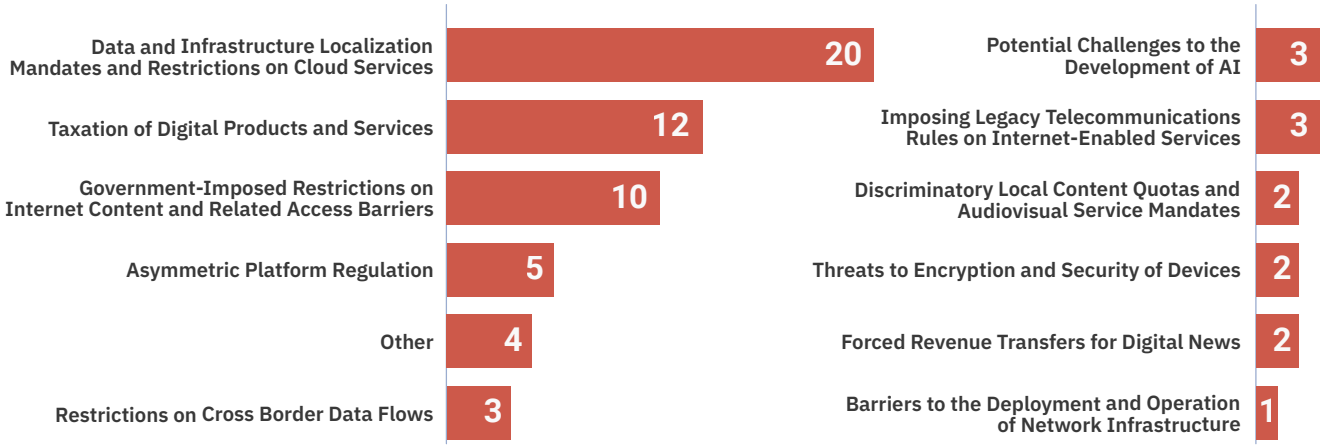
This accompanies CCIA's annual National Trade Estimate Report filing. Information and data is current as of October 30, 2025. For more, visit: digitaltradebarriers.ccianet.org.

The United States has long enjoyed strong diplomatic and economic relationships with the European Union. The exchange of goods and services has generated widespread benefits for both economies. Digital services in particular are a prominent generator of benefits for U.S. exports in this relationship. The U.S. generated approximately **$200 billion in exports of digitally-enabled services to the Euro area in 2024**, bringing numerous positive externalities for business operations and consumers in the region and a trade surplus of **$107.6 billion in digitally-enabled services**.

As work is done to advance this relationship, the United States and the EU should work together to ensure that parties do not restrict the ability of global firms to enter or expand into their markets and engage in cross-border delivery of goods and services.

This engagement comes at a critical moment in the transatlantic relationship. Through its continued pursuit of so-called "digital sovereignty," the EU has enacted policies that hinder the ability of U.S. and other foreign digital services to operate. The following is excerpted from CCIA's annual comments submitted to the Office of the U.S. Trade Representative regarding its National Trade Estimate report—including broad takeaways from the region followed by key trends.

Key Threats to the U.S.-EU trading relationship in 2025



CCIA identified

67

digital trade barriers in the European Union

41 policies enacted

26 policies in development

Digital Trade Barrier Trends for the EU in 2025

Asymmetric Platform Regulation

European Union:

- The **Digital Markets Act** imposes prescriptive obligations on "gatekeeper" platforms that overwhelmingly target U.S. technology firms, with five of six designated companies and 21 of 22 affected services being American. The measure grants the European Commission sweeping authority over product design and data-sharing, compels disclosure of proprietary information to EU rivals, and prohibits efficiency-enhancing practices. These requirements have imposed compliance costs exceeding US$1 billion annually, far above the EU's original estimates, creating discriminatory and disproportionate burdens inconsistent with fair competition principles.
- The proposed **Financial Data Access Framework** has evolved into a discriminatory barrier by excluding gatekeeper-designated companies from accessing financial data, even with explicit consumer consent. Initially intended to promote competition and innovation through data sharing across financial services, the framework now imposes a categorical restriction based on company designation rather than conduct, without justification, proportionality assessment, or avenues for appeal.

Germany:

- The 2021 reform of the **Act Against Restraints of Competition** created a new regulatory category for companies of "paramount significance for competition across markets," granting the Federal Cartel Office sweeping powers to preemptively restrict conduct such as self-preferencing or data integration and shifting the burden of proof onto targeted firms. The law has been applied exclusively to major U.S. companies. The 2023 11th Amendment further expanded the FCO's authority to impose structural remedies, presume profit disgorgement, and enforce DMA provisions, reinforcing concerns that Germany's competition regime unfairly targets U.S. firms and imposes asymmetric regulatory burdens.

Italy:

- The **Annual Competition Law** establishes a presumption that commercial users of certain digital platforms are economically dependent on those platforms, allowing the Italian Competition Authority to intervene even absent a formal proceeding. The law identifies behaviors such as restricting competition, imposing unreasonable conditions, or providing inadequate service information as presumptively abusive, creating broad discretion for enforcement.

Barriers to the Deployment and Operation of Network Infrastructure

European Union:

- The draft **Space Act** would establish an asymmetric regulatory framework that subjects non-EU satellite operators to burdensome registration through an EU-run Compliance Board while allowing EU firms to register via their Member States. By defining "giga-constellations" as systems with over 1,000 satellites, a threshold that primarily captures U.S. providers, the proposal imposes discriminatory compliance obligations and may further restrict market access by reserving certain communications services for EU-headquartered operators.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Croatia:

- Croatia's **Public Procurement Act** and **related ICT policies** create substantial barriers for foreign suppliers by requiring tender documentation in Croatian and mandating compliance with EU-specific standards such as CE marking and data residency rules. Combined with the government's reliance on the state-owned APIS IT and its Shared Services Centre for nearly all public sector infrastructure, these measures effectively exclude U.S. cloud providers from Croatia's public procurement market.

Cyprus:

- Strict **data sovereignty and residency requirements** force cloud providers to store and process sensitive data locally within Cyprus or the EU, effectively excluding U.S. firms without local infrastructure. These mandates, reinforced through public procurement contracts in sectors such as healthcare and finance, create significant market access barriers that may conflict with Cyprus's GATS commitments on cross-border computer services.

Czech Republic:

- Czech law requires cloud providers to register under a national **Cloud Computing Catalog**, creating burdensome procedures that favor domestic competitors. The forthcoming **Cybersecurity Act**, implementing the EU NIS 2 Directive, could further restrict foreign participation by classifying public administration data as critical and requiring local data storage.

European Union:

- The **Cybersecurity Certification Scheme for Cloud Services** poses a potential trade barrier as member states consider reintroducing discriminatory eligibility rules favoring EU-based providers. Although earlier drafts removed explicit nationality-based restrictions, ongoing efforts by France and Germany to revise the Cybersecurity Act to promote a "sovereign cloud" risk reviving protectionist requirements that would exclude U.S. firms from certification and distort competition in the European cloud market.
- The proposed **Cloud and AI Development Act** would establish a European-only cloud infrastructure for public services and critical sectors, reinforced by the NIS2 Directive's authority to require certified providers. By promoting a restrictive notion of "sovereign cloud" and linking certification to European infrastructure, the measure would effectively exclude U.S. cloud providers from serving key markets and create a discriminatory, closed ecosystem under the banner of digital sovereignty.
- The broader **"de-risking" agenda** and plans for European preference in public procurement aim to reduce dependence on foreign ICT suppliers, many of which are U.S. companies. These initiatives, covering technologies such as cloud computing, AI, and cybersecurity, risk introducing discriminatory procurement rules and market access restrictions that favor European providers in the name of strategic autonomy and economic security.

France:

- The **SecNumCloud certification scheme** imposes nationality-based ownership and control restrictions that explicitly exclude non-EU cloud providers from serving the public sector and operators of vital services. The framework requires EU-based headquarters, caps foreign ownership at 24%, and bans veto rights for non-EU entities, with certification now mandatory for public tenders. These provisions violate France's WTO GPA and GATS obligations and create a de facto barrier to U.S. cloud providers' participation in the French market. The 2024 **Law to Secure and Regulate the Digital Environment** introduces fines for alleged unfair practices by cloud service providers and lawmakers seek to amend it to extend SecNumCloud certification to non-European providers hosting sensitive or health-related data for public authorities. This expansion would deepen existing discrimination against U.S. firms.

- **Greece:**
  - Greece's Ministry of Finance has made participation in the **EU Code of Conduct on Data Centre Energy Efficiency** a mandatory requirement for data centers involved in Recovery and Resilience Facility–funded projects. By converting a voluntary EU standard into a binding procurement condition, Greece effectively excludes U.S. cloud providers whose facilities meet equivalent international certifications, creating a discriminatory market access barrier and undermining fair competition in EU-funded digital projects.

- **Hungary:**
  - The **Electronic Information Security of State and Local Government Bodies Act** imposes strict data localization requirements for public sector and critical service providers, mandating that data be stored and processed within the European Economic Area. Non-Hungarian providers must appoint a local representative to ensure compliance, effectively excluding U.S. cloud and IT service providers without EEA-based infrastructure and creating a significant barrier to cross-border data services.

- **Ireland:**
  - Ireland's grid maintains a **de facto moratorium on new data center grid connections**, citing energy security concerns and effectively halting expansion by U.S. investors despite the root issue being inadequate grid infrastructure. The resulting regulatory paralysis has deterred investment and undermined Ireland's role as a digital infrastructure hub. In parallel, a 2024 effort to create a **national cloud procurement framework** collapsed after Irish authorities imposed terms that excluded U.S. providers, reportedly due to concerns over the U.S. CLOUD Act.

- **Italy:**
  - The Ministry of Culture's expansive interpretation of Italy's **Cultural Heritage Code** classifies public archives, including school and educational records, as "cultural heritage," prohibiting their storage or processing outside Italy. This restrictive approach, lacking alignment with contemporary cloud practices, creates a major barrier for foreign—particularly U.S.—cloud providers seeking to serve Italy's education sector.

- **Malta:**
  - Malta's Gaming Authority imposes **stringent data mirroring requirements** on all licensed gaming providers, mandating that essential or regulatory data—such as player information, financial transactions, and activity logs—be continuously replicated on live servers located in Malta when primary servers are hosted abroad. These obligations, justified as necessary for real-time regulatory access and supervision, require companies to provide detailed documentation on server locations and data transfer processes, ensuring the MGA can access mirrored data at any time. While formally nationality-neutral, these rules disproportionately burden non-EU and U.S. operators relying on global cloud infrastructure.

- **Poland:**
  - Poland is advancing a **draft cybersecurity law** that would expand the authority of the Minister of Digital Affairs to designate "High Risk Vendors" (HRVs). Companies designated as HRVs would be required to remove their equipment or software from critical infrastructure systems within a specified timeframe. The proposal's broad and ambiguous criteria for designation raise serious concerns about arbitrary enforcement and disproportionate impact on non-EU providers, particularly U.S. technology firms.

Discriminatory Local Content Quotas and Audiovisual Service Mandates

- **Germany:**
  - The proposed **Investment Obligation Act** would require large streaming and digital service providers to reinvest up to 10% of their locally generated revenue into German or European audiovisual productions. Framed as a cultural policy to support the domestic film and television industry, the measure effectively imposes a mandatory local content levy that disproportionately impacts U.S. streaming services, particularly those operating on licensing rather than production models.

- **Italy:**
  - Italy's **implementation of the EU AVMS Directive (Directive 2018/1808)** through a Legislative Decree introduced mandatory investment quotas requiring audiovisual service providers to reinvest up to 25% of their annual net revenues in European, primarily Italian, works, later reduced to 20% in 2024. These high quotas significantly raise costs for international streaming platforms, particularly U.S. providers.

Forced Revenue Transfers for Digital News

- **European Union:**
  - The **European Media Freedom Act** introduces special treatment for media content on very large online platforms, creating overlap and potential conflicts with the Digital Services Act. Its implementation risks adding regulatory complexity and uncertainty for U.S. digital services, underscoring the need for U.S. engagement to ensure that new rules complement rather than duplicate existing frameworks.

- **France:**
  - France's **implementation of Article 15 of the EU Copyright Directive** created a press publishers' right requiring platforms to pay for displaying news content, leading to repeated enforcement actions against U.S. firms. After Google adjusted search displays instead of entering licensing deals, France's competition authority ordered payments to publishers in 2020 and later fined Google €500 million in 2021 for allegedly failing to negotiate in good faith, reinforcing France's aggressive and discriminatory application of EU copyright rules toward U.S. digital platforms.

Government-Imposed Content Restrictions and Related Access Barriers

- **Czech Republic:**
  - The implementation of the EU Copyright Directive introduces discriminatory obligations on "dominant" firms under **Amendment 1274** and grants the Ministry of Culture broad powers to set remuneration and demand company data without IP safeguards, with penalties up to 1% of global turnover. Additional provisions under **Article 51a** could allow local entities to block U.S. services for content moderation decisions, undermining online platforms' ability to combat misinformation and conflicting with EU court rulings on freedom of expression protections.

- **European Union**
  - The **Digital Services Act** imposes extensive due diligence, transparency, and auditing requirements on online platforms, with the most burdensome obligations falling on very large U.S. firms. By regulating based on size rather than risk, the DSA disproportionately affects American companies, while its broad scope, covering issues from targeted advertising to age verification, extends far beyond online safety. High compliance costs, intrusive audit demands, and overlapping obligations under related measures like the **General Product Safety Regulation** further increase regulatory fragmentation and create substantial barriers for U.S. digital service providers.

- The proposed **Regulation to Prevent and Combat Child Sexual Abuse** would mandate online service providers to detect, report, and remove child sexual abuse material and grooming in real time, including through scanning private communications. The proposal's broad scope and detection requirements risk undermining end-to-end encryption and creating intrusive surveillance obligations, raising strong opposition from privacy regulators, civil society, and industry. While a temporary derogation from the e-Privacy Directive allowing voluntary detection remains in force until April 2026, ongoing legislative uncertainty leaves U.S. service providers exposed to conflicting compliance pressures and privacy risks.
- The **Regulation on Transparency and Targeting of Political Advertising** imposes strict labeling, targeting, and amplification requirements that exceed those under the Digital Services Act. Noncompliance can trigger fines of up to 4% of global turnover, prompting several U.S. companies to withdraw their political advertising services from the EU market due to the high compliance risks and operational burdens.
- The **EU Copyright Directive** imposes press publisher rights and filtering obligations under Articles 15 and 17 that diverge sharply from global IP norms and disproportionately burden U.S. online services. Its vague "best efforts" standard, fragmented national implementation, and limited exceptions create high compliance costs and legal uncertainty, undermining user-generated content and text and data mining. Further, 2024 **revisions to the Digital Services Act** extend liability for defective products to online marketplaces and software providers, reversing the burden of proof.

France:

- In 2023, the government **banned the use of messaging applications** such as WhatsApp, Telegram, and Signal for official communications, mandating the use of domestic alternatives Olvid and Tchap. Although justified on security grounds, the decision lacked evidence of actual vulnerabilities and effectively favored French-developed services, raising concerns of discriminatory treatment and potential noncompliance with France's WTO GPA obligations.

Germany:

- The **Network Enforcement Law (NetzDG)** requires social media platforms to remove "manifestly unlawful" content within 24 hours or face fines of up to €50 million. The law's vague definitions and heavy penalties have prompted over-removal of lawful content, raising serious concerns about transparency, proportionality, and freedom of expression. Amendments enacted in 2022 further expanded takedown obligations before being partially suspended for violating EU civil liberties rules, while the law's influence has spread globally, inspiring restrictive content regimes in other countries.

Italy:

- The **"Piracy Shield" platform** enables rightsholders to secure rapid ISP blocking orders for allegedly infringing content within 30 minutes via an automated system overseen by AGCOM. While aimed at combating online piracy, the system has caused widespread overblocking of lawful content, disrupting legitimate services. In 2025, Italian authorities proposed amendments to expand the platform's use. Despite minor adjustments, concerns persist that the Piracy Shield regime continues to endanger lawful online activity and information access.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

European Union:

- The exploration of potential **network usage fees** has evolved into a significant potential trade barrier that would require "large traffic generators," primarily U.S. content and application providers, to pay European telecom operators for delivering their traffic. Despite overwhelming stakeholder opposition and findings from BEREC confirming such fees would violate net neutrality and harm innovation, the Commission continues

to pursue the idea through follow-on initiatives like the forthcoming **Digital Networks Act**. The proposal, estimated by incumbents to generate €20 billion annually, would distort competition by forcing U.S. firms to subsidize European ISPs, undermining open internet principles and equitable market access.

- **Italy:**
  - Italy's telecom regulator recently introduced a dispute resolution mechanism that could pave the way for **network usage fees** long sought by European telecom operators. This framework risks enabling paid peering arrangements that would dismantle the settlement-free internet model and impose discriminatory costs on CAPs and CDNs, particularly U.S. providers.

Potential Challenges to the Development of AI

- **European Union:**
  - The **AI Act** establishes a risk-based framework regulating AI systems across all sectors but creates substantial compliance burdens and uncertainty for U.S. and global firms. Delayed harmonized standards, dual compliance risks with ISO frameworks, and extensive training data disclosure requirements expose companies to trade secret and copyright risks, while broad definitions of "high-risk" and "general-purpose" AI introduce ambiguity and administrative complexity. With fines reaching 7% of global turnover and unclear allocation of responsibilities, the Act risks discouraging AI innovation and investment in Europe.

Restrictions on Cross-Border Data Flows

- **European Union:**
  - The **General Data Protection Regulation** has created significant compliance burdens and legal uncertainty for U.S. companies, particularly small and mid-sized exporters. Layered with additional EU rules such as the Digital Markets Act, Data Act, and Digital Services Act, the framework imposes overlapping and asymmetric obligations that raise costs and deter innovation. Persistent instability in transatlantic data transfers, coupled with expansive enforcement powers, retroactive liability, and high penalties of up to 4% of global turnover, has further undermined predictability and market access.
  - The **Data Act** and the **Data Governance Act** establish overlapping and restrictive frameworks that limit how data generated within the EU can be accessed, transferred, and shared. The Data Act prohibits U.S. gatekeepers from receiving IoT data, restricts cross-border transfers, and requires disclosure of proprietary information, while the DGA extends similar controls to non-personal and industrial data. Together, these measures create a fragmented, high-cost compliance environment that disadvantages U.S. companie.

Taxation of Digital Products and Services

- **Austria:**
  - Austra's **5% DST** on digital advertising services applies to companies with global revenues above €750 million while largely excluding domestic suppliers. The measure was explicitly aimed at foreign providers, particularly large U.S. platforms, and raised €103 million in 2023, with most payments coming from foreign firms.

- **Belgium:**
  - In 2025, Belgium announced plans to introduce a **3% DST** by 2027, pending the outcome of European and international negotiations. Modeled on its 2019 proposal, the measure would target companies with global revenues above €750 million and local revenues above €5 million, imposing new tax burdens on foreign digital service providers, particularly U.S. firms.

- **Croatia:**
  - Croatia announced plans in 2022 to introduce a **DST** modeled on Austria's, which would disproportionately impact U.S. digital service providers.

- **Czech Republic**
  - The Czech government proposed a **7% DST** in 2019 targeting firms with global revenues above €750 million and domestic revenues over CZK100 million.

- **France:**
  - France's **3% DST** targets revenues from digital intermediation and advertising services, explicitly designed to target major U.S. technology firms while excluding most French competitors. It has generated over $3 billion, primarily from U.S. companies, and is projected to yield €800 million in 2024. Lawmakers are now considering raising the rate to 15% and narrowing the scope to capture only five U.S.-based firms, further entrenching its discriminatory character.
  - France's **video content tax** on cross-border streaming and video-sharing platforms, as well as a **2024 levy of 1.2% on music streaming and social media revenues**, have directed proceeds to domestic cultural funds while creating overlapping tax burdens. The government has further proposed a **1.3% levy on Very Large Online Platforms**, compounding existing turnover-based taxes and explicitly aiming to make U.S. firms contribute disproportionately to subsidizing French industries.

- **Germany:**
  - Germany has announced plans for a **10% digital levy** on large platforms that distribute or monetize media and cultural content, modeled in part on Austria's Digital Services Tax. Although still at the proposal stage, the measure would impose one of the highest digital taxes in Europe and disproportionately affect U.S. technology firms operating in Germany's online media market.

- **Italy:**
  - Italy's **3% DST** applies to revenues from digital advertising, multilateral interfaces, and user data transmission for firms with over €750 million in global and €5.5 million in local revenues. The tax disproportionately targets U.S. companies and was explicitly designed by senior officials to capture large U.S. tech firms. While Italy agreed to phase out the DST under the OECD Two-Pillar framework, the government has signaled plans to retain or expand it if Pillar 1 negotiations fail. As of 2024, Italy has collected approximately $1.8 billion, mostly from U.S. firms, underscoring the discriminatory impact of this measure.

- **Poland:**
  - Poland's government is proposing a **DST** that would impose turnover-based levies of 3–7.5% on digital sectors such as e-commerce, search, and online advertising, disproportionately burdening foreign, particularly U.S., providers while exempting domestic competitors. The "wide" and "narrow" variants are estimated to raise US$470–930 million and US$130–200 million annually, respectively, with revenues directed to a discretionary fund to support Polish tech and media firms. By taxing digital but not equivalent offline activities and applying higher rates to sectors dominated by U.S. companies, the measure embeds structural discrimination and mirrors DSTs in France and the UK.

- **Spain:**
  - Spain imposes a **3% DST** on revenue from online advertising, the sale of user data, and digital intermediation services, applying to firms with global revenue above €750 million and local revenue above €3 million. Between 2021 and 2024, the measure generated over US$1 billion—largely from U.S. firms explicitly referenced during legislative debate.

Threats to the Security of Devices and Services

European Union:

- The **Network and Information Security Directive** imposes extensive cybersecurity and reporting obligations on essential service providers, including cloud and data center operators, and could make certification under the EU Cybersecurity Act effectively mandatory. Previous drafts of the associated certification scheme contained discriminatory provisions against non-EU providers, and overly low incident reporting thresholds risk excessive administrative burdens. Delayed national transposition and uneven implementation further amplify compliance uncertainty for U.S. firms.
- The **EU's Cyber Resilience Act** introduces broad pre-market approval requirements for digital products and services, creating long delays and new compliance costs for technology exporters. By mandating vulnerability disclosures to national authorities within 24 hours, before fixes are developed, the measure diverges from global best practices and could unintentionally heighten security risks while imposing disproportionate burdens on U.S. hardware, software, and cloud providers.