Key Threats to Digital Trade 2025

Middle East & Africa

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.

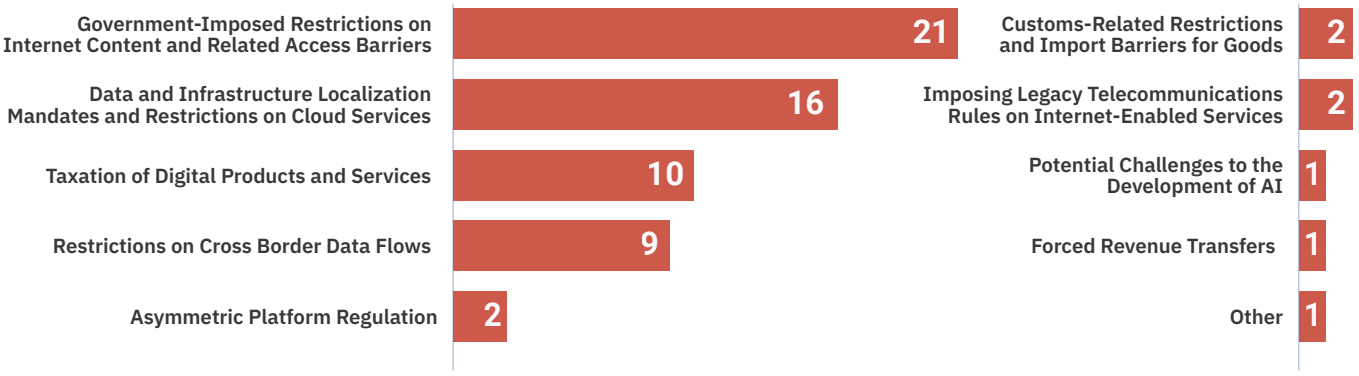
The United States has enjoyed strong diplomatic and economic relationships with countries in the Middle East and Africa for decades. Services drive the modern benefits for U.S. exports in this mutually beneficial relationship, as are digital services. The U.S. generated at least **$18 billion in exports of digitally-deliverable services** to leading markets in the Middle East and Africa in 2022, bringing numerous positive externalities for business operations and consumers in the region.

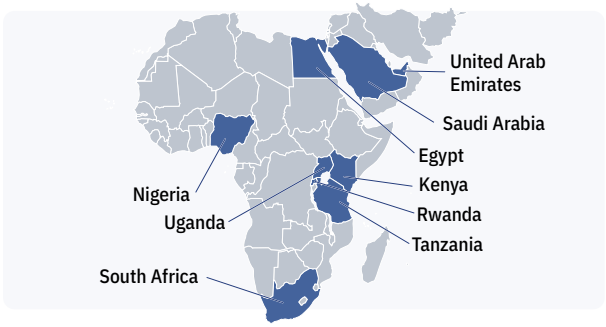
This region includes an analysis of policies in Egypt, Kenya, Nigeria, Rwanda, Saudi Arabia, South Africa, Tanzania, Uganda, and the United Arab Emirates (UAE).

The United States has formalized its trading partnership and economic cooperation with countries in the region in several fora, several bilateral treaties, and prior work around the Middle East Free Trade Area Initiative. As work is done to advance these initiatives, the U.S. should ensure partners do not restrict the ability of U.S. 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 relationship. Countries in the Middle East and Africa have enacted policies that hinder the ability of U.S. 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 details of key trends.

Key Threats to the U.S.-Middle East & Africa trading relationship in 2025





CCIA identified

65

digital trade barriers in the Middle East & Africa region

49 policies enacted

16 policies in development

Digital Trade Barrier Trends for the Middle East & Africa in 2025

Asymmetric Platform Regulation

Kenya:

- Proposed amendments to the **Competition Act** that would introduce a new "abuse of superior bargaining position" standard, replacing the current focus on "abuse of power." This shift would allow the Authority to challenge transactions even in the absence of demonstrable harm to competition or consumers, creating broad discretionary powers and significant legal uncertainty.

Saudi Arabia:

- Saudi Arabia's draft **Competition Regulations for Digital Content Platforms** propose broad and unclear rules for large online services, including arbitrary thresholds and vague prohibitions on "anti-competitive" self-preferencing. Though not yet adopted, these measures could restrict innovation and market access for U.S. firms, prompting industry calls for close monitoring of their potential impact.

Customs-Related Restrictions and Import Barriers for Goods

Egypt:

- Egypt's import regime suffers from **inconsistent customs valuation practices, arbitrary tariff reclassifications, and opaque administrative procedures** that inflate costs and undermine predictability for traders. Combined with burdensome registration and permanent establishment requirements under the **Simplified Vendor Registration System**, these measures create significant barriers for cross-border e-commerce.

Data and Infrastructure Localization Mandates and Restrictions on Cloud Services

Kenya:

- The **Data Protection Act** empowers the Cabinet Secretary under Section 50 to determine categories of personal data that must be stored and processed domestically to protect national interests. In practice, the Data Protection Regulations of 2020 have been interpreted to require localization of a wide range of data, including civil registration, education, payment systems, revenue, and health data, obliging companies to store at least one copy in a Kenyan data center.
- The **Computer Misuse and Cybercrimes Act of 2018** and its **2024 implementing regulations** impose strict data localization and reporting obligations on operators of "Critical Information Infrastructure," including cloud service providers. Covered entities must establish domestic Cybersecurity Operations Centers to monitor and report compliance to the Communications Authority, creating costly, duplicative infrastructure and operational burdens.
- **Kenya's Cloud Policy** mandates that all public entities prioritize local cloud solutions for government ICT projects and upgrades. While promoted as a tool for digital sovereignty, the policy's preference for government-approved providers based in Kenya effectively excludes or disadvantages foreign cloud suppliers.

Nigeria:

- The 2019 **Guidelines for Nigerian Content Development in ICT** require all "sovereign data," broadly defined to include government information and data managed by information service providers, to be stored domestically, creating a de facto data localization mandate. In 2023, the previous administration advanced two complementary proposals: the **NITDA Bill**, which would expand NITDA's authority over digital service providers, extend its 1% levy on foreign platforms, and grant oversight of the telecom sector; and the

National Shared Services Corporation (NSSC) Bill, which would consolidate ICT infrastructure and cloud services for federal agencies under a state-owned entity. Although both bills stalled before the elections, their revival would raise concerns about state control over ICT infrastructure, discriminatory taxation, and market entry barriers.

Saudi Arabia:

- Saudi Arabia's cloud and data regulations impose strict localization mandates and extensive government control over digital infrastructure, requiring most data and cybersecurity operations to remain within the country. Recent consultations by the **Saudi Data & AI Authority** further expand compliance and registration obligations, potentially introducing new protectionist barriers and increasing operational burdens for foreign cloud and digital service providers.

South Africa:

- The **National Data and Cloud Policy**, published on May 31, 2024, mandates that "data that incorporates content pertaining to the protection and preservation of **national security and sovereignty** of the Republic shall be stored only in digital infrastructure located within the borders of the Republic." Industry concern centers on the **unclear scope of covered data**, fearing a broad interpretation that would impose extensive local storage requirements on companies operating in the market.

Uganda:

- While Uganda's **Computer Misuse Act** does not explicitly mandate data localization, the **Bank of Uganda** has interpreted it to require financial institutions operating in the country to **store customer digital financial information on domestic data centers**. This interpretation imposes a de facto localization requirement to enable the government to compel real-time data collection or recording by service providers.

United Arab Emirates (UAE)

- The UAE Cybersecurity Council mandates that federal and Emirate-level data workloads, along with data for financial services and healthcare, must be **hosted on servers within the UAE**.
- The government imposes strict sovereignty controls, requiring cloud services for the public sector and regulated industries to be solely subject to **UAE law**, not foreign jurisdiction, and to **physically localize** data centers and all associated operations and personnel.
- The **National Cloud Security Policy** formalizes this by requiring Secret and Top Secret data to be stored in fully sovereign infrastructure under exclusive UAE jurisdiction, though it offers clearer compliance pathways for foreign providers willing to localize.

Government-Imposed Content Restrictions and Related Access Barriers

Egypt:

- The Supreme Council for Media Regulation, established under **Law No. 180** of 2016, imposes extensive licensing and compliance obligations on media and online platforms, including mandatory local representation, high licensing fees, and 24-hour content removal requirements. Recent enforcement measures backed by the NTRA and Central Bank of Egypt have increased compliance risks for unlicensed platforms, while the alternative accreditation model under Decree No. 92 of 2020 remains underutilized. These measures create significant operational and financial burdens for U.S. digital service providers and restrict market access through unclear procedures and selective enforcement.

- In 2025, Egyptian security agencies intensified **enforcement actions against content creators** under the guise of addressing national security concerns, including arrests and heightened scrutiny of platforms following high-profile incidents. While framed as efforts to preserve public order and social stability, these actions contribute to a restrictive operating environment for online platforms and exacerbate risks of arbitrary enforcement and censorship.

Kenya:

- **Nationwide internet restrictions** during 2024 protests cut connectivity by 40 percent across major networks and costing the economy an estimated US$6.3 million in GDP losses per day. These shutdowns, implemented despite prior government assurances against such actions, disrupted all major telecommunications providers and raised serious concerns about freedom of expression and the reliability of Kenya's digital infrastructure. In 2025, similar protests prompted bans on live broadcasting and the temporary suspension of several media outlets, though these measures were later overturned by the High Court, underscoring ongoing tensions between state control and media freedom.
- The draft **Computer Misuse and Cybercrime Bill**, which would grant the National Computer and Cybercrimes Coordination Committee sweeping authority to block websites and applications promoting broadly defined "illegal activities" or "extreme religious and cultic practices." The Bill's vague language and lack of procedural safeguards create a high risk of misuse to suppress dissent and restrict online speech. If enacted, the measure could expand state control over digital communications, heighten compliance risks for service providers, and further undermine Kenya's reputation as an open and predictable digital market.

Nigeria:

- The 2022 **Code of Practice for Interactive Computer Service Platforms** and Internet Intermediaries requires digital platforms with more than one million users to incorporate locally and maintain a physical presence in Nigeria, as well as appoint a local liaison officer, measures that restrict cross-border service provision and increase compliance costs for foreign firms. It also mandates content moderation processes, notice-and-takedown procedures, transparency reporting, and cooperation with government data and content requests. While subsequent revisions relaxed some provisions, such as criminal liability, "stay-down" requirements, and takedown timelines, the framework continues to create significant operational burdens and limits market access for U.S. digital service providers.
- A 2022 amendment to Nigeria's advertising laws expanded the **Advertising Regulatory Council of Nigeria's pre-approval mandate** to include all online advertising, extending a regime previously limited to traditional media. This requirement has proven unworkable for global digital platforms that depend on dynamic, automated ad placement systems. In October 2022, ARCON fined Meta $70 million for allegedly running ads without prior approval and later pursued similar fines against TikTok and Google. Although ARCON's enforcement remains largely symbolic—the Meta lawsuit was eventually withdrawn after years of inaction—the policy introduces persistent legal uncertainty and excessive compliance risks for foreign platforms. The pre-approval requirement effectively restricts digital advertising operations.

Saudi Arabia:

- Saudi Arabia maintains broad control over online speech via the **2007 Anti-Cyber Crime Law** and proposed measures that would increase platform liability and content control.
- The proposed **Media Law** would require licenses for "media activity" by platforms and users, while the draft **CST Global Digital Content Safe Harbor Law** offers platform liability exemptions only with a government-issued and revocable certification.
- The **Deepfake Guidelines** instruct platforms to proactively detect and prevent misleading deepfake content, and a proposed amendment to the **Telecommunications and Information Technology Act** could impose severe fines and service blocking on platforms that fail to implement internet filtering.

- The government heavily restricts encrypted Voice over Internet Protocol (VoIP) services on global apps like WhatsApp to protect domestic telecom revenue and for security/monitoring purposes, and the **Saudi Central Bank (SAMA)** has directed financial institutions to stop using third-party instant messaging apps for official customer communications.

Tanzania:

- Tanzania's Communications and Regulations Authority (TCRA) has imposed a **VPN-ban**, requiring users to declare their use and provide IP addresses to the government under **Regulation 16(2) of the Electronic and Postal Communications (Online Content) Regulations of 2020**. Furthermore, the government has escalated blocks on online platforms, compelling ISPs to block access to platforms like **X** and forcing social media companies to suspend accounts for publishing "restricted content," particularly during periods of political unrest.

United Arab Emirates (UAE)

- The UAE maintains longstanding regulatory restrictions on unlicensed **Voice over Internet Protocol (VoIP)** services, selectively blocking the voice and video features of popular foreign platforms like WhatsApp and FaceTime, which protects the revenue of the state-licensed telecom duopoly and allows for government control over communications.
- The **2018 National Media Council Content Creators law** imposes onerous licensing requirements on a broad scope of social media influencers, including foreign residents and those with paid associations, which creates unnecessary friction and a potential selective enforcement mechanism inhibiting digital trade.

Imposing Legacy Telecommunications Rules on Internet-Enabled Services

Kenya:

- In April 2024, the Communications Authority of Kenya issued a **Programming Code for Broadcasting Services** and directed major digital companies to comply, followed by four **additional regulations from the Film and Classification Board** on July 26, 2024, targeting OTT service providers. Neither agency has legal authority under existing law to regulate OTT platforms, raising serious concerns about regulatory overreach and duplication. Applying broadcasting-style obligations to OTT services would create disproportionate compliance costs.

Restrictions on Cross-Border Data Flows

Egypt:

- **Personal Data Protection Law No. 151/2020** establishes an exceptionally restrictive cross-border data transfer regime that combines discretionary adequacy assessments with mandatory PDPC licensing. Transfers are prohibited unless the destination country meets Egypt's protection standards and a permit is obtained, with no published adequacy list and burdensome documentation requirements. Severe penalties, combined with opaque determinations and a lack of mutual recognition mechanisms, create high compliance costs and legal uncertainty.

Kenya:

- The **2020 ICT Policy** includes a requirement that all Kenyan data be stored within the country, conflicting with the 2019 Data Protection Act, which allows cross-border data transfers subject to safeguards determined by the Data Commissioner.

- **Nigeria:**
  - The **Data Protection Act** imposes strict conditions on cross-border data transfers, allowing them only when the recipient country or organization provides an adequate level of protection through legal frameworks, binding corporate rules, or contractual safeguards. Data controllers must document all transfers and protective measures, while the Nigeria Data Protection Commission can restrict specific data categories or issue adequacy determinations by country or sector. Complementing this, the 2023 **Guidelines for Content Development in Information and Communication Technology** mandate local hosting of government, consumer, and subscriber data, reinforcing localization trends. **Additional sectoral rules**, such as the 2011 telecom guidelines requiring domestic hosting of subscriber data and the Central Bank's card transaction routing rules, further limit data mobility. Collectively, these overlapping mandates create legal uncertainty and raise operational costs for foreign cloud, payment, and telecom providers.

- **Saudi Arabia:**
  - Saudi Arabia's **Personal Data Protection Law (PDPL)**, despite recent amendments aimed at easing restrictions, remains a significant digital trade barrier due to a lack of clarity regarding exceptions for data transfers and the scope of jurisdictions deemed adequate for data flows. Further concerns stem from vague definitions like "public interest" in the **Risk Assessment Guidelines for Transferring Personal Data outside the Kingdom**, and potential new legal ambiguities in draft amendments to the **Implementing Regulation of the PDPL**, which complicate compliance obligations for foreign digital service providers.

Taxation of Digital Products and Services

- **Kenya:**
  - The **2020 tax reforms** introduced multiple measures targeting digital trade: a 20% withholding tax on marketing and advertising services provided by non-residents, a 1.5% DST on income from digital marketplaces, and a revision to VAT rules on exported services—initially exempted but restored to zero-rated status in 2023. While the VAT correction reduced distortion for local exporters, the overlapping DST and withholding obligations continue to impose disproportionate administrative burdens on cross-border digital services providers. The 2024 **Tax Laws (Amendment) Act** and the **Tax Procedures (Amendment) (No. 2) Act**, replacing the 1.5% DST with a 3% Significant Economic Presence Tax on non-resident digital platform operators. The Acts also expanded the definition of "royalty" to include nearly all software-related payments and imposed a 20% withholding tax on digital marketplace transactions, along with excise duties on digital services. These overlapping and unpredictable measures deviate from international tax norms, risk double taxation, and disproportionately burden foreign digital suppliers.

- **Nigeria:**
  - The 2021 **Finance Act** introduced new income tax and digital services obligations for non-resident companies providing digital goods or services, effectively establishing a Significant Economic Presence regime. The law applies to non-resident companies earning above specified thresholds and targets firms generating revenue from Nigerian users, collecting data on them, or offering local payment options. While framed as a general tax reform, its design and application have disproportionately affected U.S. multinationals. The Act also expanded Nigeria's VAT framework to digital transactions, resulting in a 7.5 percent VAT for major U.S. firms. Under the SEP regime, non-resident digital service firms may be taxed on a deemed profit basis, leading to an effective rate of roughly 6% on turnover. Together, these measures create overlapping and discriminatory fiscal burdens on cross-border digital suppliers.

- **Rwanda:**
  - On May 27, 2025, the Government of Rwanda passed a law implementing a **1.5% digital service tax (DST)** on digital service providers with significant operations in the country. Key details, including the scope of the tax and what constitutes "substantial national presence," will be specified in a forthcoming **Ministerial Order**.

- **Saudi Arabia:**
  - Although Saudi Arabia does not have a standalone digital services tax, it imposes a broad **15% VAT** on non-resident digital service providers selling to Saudi customers. Recent amendments to the **VAT Implementing Regulations** require electronic platforms acting as intermediaries to collect the VAT, manage compliance documentation, and fulfill reporting obligations, significantly increasing the administrative and compliance burdens on foreign digital companies.

- **Tanzania:**
  - Tanzania adopted a **2% DST** as part of its 2022-2023 Budget, which is imposed on revenue made by any non-resident person soliciting a Tanzanian-sourced payment from an individual. The DST does not include a minimum threshold, subjecting U.S. companies to the tax from the first dollar of in-scope revenue.

- **Uganda:**
  - The Ugandan government adopted a **5% DST**, effective July 1, 2023, on revenue earned by non-residents offering a wide range of digital services, including online advertising, data, content, and cloud computing, to Uganda-based consumers. The law acts as a barrier because it does **not include a minimum threshold**, subjecting U.S. digital service providers to the tax from the first dollar of in-scope revenue.

Potential Challenges to the Development of AI

- **Saudi Arabia:**
  - Saudi Arabia's AI regulatory framework remains nascent, emphasizing innovation and ethical use through sectoral guidelines rather than comprehensive legislation. However, the draft **Global AI Hub Law** (May 2025) introduces "AI Hubs" or sovereign data zones with unclear data protection, jurisdictional, and oversight rules, creating uncertainty for cross-border operations.

Forced Revenue Transfer for Digital News

- **South Africa:**
  - The updated draft **White Paper on regulating Audio and Audiovisual Media Services and Online Content Safety**proposes introducing a **licensing fee** for online platforms, the nature of which will be determined by the Independent Communications Authority of South Africa (ICASA), which will also consider local content quotas.
  - The provisional report from the **Media and Digital Platforms Market Inquiry (MDPMI)** recommends trade-distortive remedies, including a **1% copyright levy**, **mandatory annual payments** from American companies to publishers for linking to news, and a potential **5-10% digital levy** on digital advertising revenue.