

Cyber Sovereignty

International Security, Mass Communication, and the Future of the Internet

The internet has become a battleground for global power struggles, with nations and even terrorist organizations wielding cyber-attacks to exert control. As the absence of binding international laws and norms leaves cyberspace largely unchecked, countries are seeking to establish their Sovereign Cyber Domains (SCD) - tightly controlled cyberspaces. In this illuminating monograph, the author explores how Russia, China, Iran, and others perceive the internet as a means for the United States and its allies to maintain global dominance and influence foreign audiences, driving their pursuit of strict regulations over domestic cyber affairs and mass communication. Yet, even the United States is now susceptible to foreign cyber operations, mainly foreign influence that undermines its domestic affairs.

Even International Blocs like the European Union had expressed concerns about foreign influence and privacy rights abuses, leading to regulatory initiatives like the General Data Protection Regulation, Digital Services Act and the Digital Markets Act. As nations prioritize cybersecurity and sovereignty over free speech and convenience, the book predicts a future of increased regulation across all layers of the cyber domain, mirroring the historical emergence of the concept of sovereignty.

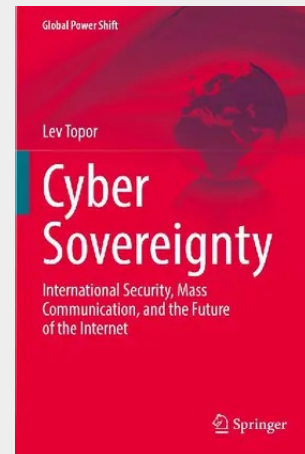
Drawing on a combination of political science, international relations, and cyber domain practices, this monograph offers valuable insights for policymakers, practitioners, researchers, and students. By analyzing existing cyber sovereignty processes and predicting future trends, the book contributes to international relations theories, sheds light on the challenges of an unregulated cyber domain, and provides guidance for a secure and controlled digital future.

Recipient of the Israel Political Science Association (ISPSA) Annual Best Book Award.

The internet has become a battleground for global power struggles, with nations and even terrorist organizations wielding cyber-attacks to exert control. As the absence of binding international laws and norms leaves cyberspace largely unchecked, countries are seeking to establish their Sovereign Cyber Domains (SCD) - tightly controlled cyberspaces. In this illuminating monograph, the author explores how Russia, China, Iran, and others perceive the internet as a means for the United States and its allies to maintain global dominance and influence foreign audiences, driving their pursuit of strict regulations over domestic cyber affairs and mass communication. Yet, even the United States is now susceptible to foreign cyber operations, mainly foreign influence that undermines its domestic affairs.

Even International Blocs like the European Union had expressed concerns about foreign influence and privacy rights abuses, leading to regulatory initiatives like the General Data Protection Regulation, Digital Services Act and the Digital Markets Act. As nations prioritize cybersecurity and sovereignty over free speech and convenience, the book predicts a future of increased regulation across all layers of the cyber domain, mirroring the historical emergence of the concept of sovereignty.

Drawing on a combination of political science, international relations, and cyber domain practices, this monograph offers valuable insights for policymakers, practitioners, researchers, and students. By analyzing existing cyber sovereignty processes and predicting future trends, the book contributes to international relations theories, sheds light on the challenges of an unregulated cyber domain, and provides guidance for a secure and controlled digital future.



128,39 €

119,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783031582011

Medium: Buch

ISBN: 978-3-031-58201-1

Verlag: Springer

Erscheinungstermin: 28.06.2025

Sprache(n): Englisch

Auflage: Erscheinungsjahr 2025

Serie: Global Power Shift

Produktform: Kartoniert

Gewicht: 353 g

Seiten: 207

Format (B x H): 155 x 235 mm

