

1. Record Nr.	UNINA9910869184103321
Autore	Topor Lev
Titolo	Cyber Sovereignty : International Security, Mass Communication, and the Future of the Internet / / by Lev Topor
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031581991 9783031581984
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (217 pages)
Collana	Global Power Shift, , 2198-7351
Disciplina	327.116
Soggetti	Security, International Politics and war International law Communication in politics International Security Studies Military and Defence Studies Public International Law Political Communication
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1. Introduction -- Chapter 2. Cyberspace: Structure, Functionality and Vulnerabilities -- Chapter 3. Sovereignty, Power, International Security and a Lack of International Law -- Chapter 4. Cyber Warfare: Global Trends and Proxy Wars -- Chapter 5. Mis/Disinformation and National Resilience: Are Countries Immune to Fake News? -- Chapter 6. Secure Cyber Domains (SCD): Mature Models -- Chapter 7. Vulnerable Models of Cyber Domains -- Chapter 8. The Future of the Internet.
Sommario/riassunto	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.
