Review – Cyber Sovereignty

https://www.e-ir.info/2024/10/27/review-cyber-sovereignty/

PNINA SHUKER, OCT 27 2024

Cyber Sovereignty: International Security, Mass Communication, and the Future of the Internet
By Lev Topor
Springer, 2024

Cyber Sovereignty is highly relevant to current geopolitical dynamics, addressing pressing issues such as cyber warfare, mis/disinformation, and the role of technology in international power struggles. Lev Topor's analysis provides valuable insights into how states navigate the complexities of the digital age and the implications for global security and stability. Beyond the technical and political analysis, Topor raises important ethical and philosophical questions about sovereignty, free speech, and the balance between security and liberty in cyberspace. The book examines the complex and evolving landscape of cyberspace and its implications for international relations, security, and governance. Toper provides a comprehensive analysis of how nation-states increasingly assert control over their digital domains, crafting tailored versions of the internet that align with their political, religious, cultural, and security agendas.

Following Chapter 1, on the methodology, arguments, and findings of the study, Topor provides a historical overview of the Internet's development from its origins as an American defense project (ARPANET) to its current status as a global communication network. This context is crucial for understanding the geopolitical power struggles around cyberspace. Topor argues that the internet, initially perceived as a tool for global unity, has become a contested space where states battle for control and influence.

Chapter 3 examines the concepts of sovereignty, power, and international security as they apply to cyberspace. Topor introduces the idea behind "cyber sovereignty," referring to nation-states' efforts to control their segment of the internet as they also control their borders. By erecting digital borders and regulating content, states aim to protect national interests and maintain social stability. The book goes on to explore examples such as China's Great Firewall, Russia's RuNet, Iran's National Information Network, and North Korea's closed cyberspace known as Kwangmyong ("bright star"), in contrast to the relatively open but vulnerable American, British, and Israeli cyberspace.

In Chapter 4, Topor delves into the realm of cyber warfare, highlighting how cyberattacks have become a new frontier in international conflict. The chapter explores 500 significant cases of cyber warfare and also dives into the details of incidents such as the Russian cyberattack on the Ukrainian power grid, the North Korean WannaCry ransomware attack, the alleged Russian cyber-attacks on American electoral processes, and more, demonstrating how cyber operations can disrupt national infrastructure and pose significant security threats. Topor underscores the importance of developing robust cybersecurity measures and international cooperation to mitigate such risks.

A significant portion of the book is dedicated to the phenomenon of mis/disinformation and its impact on national resilience. In Chapter 5, Topor asks "Are Countries Immune to Fake News? He examines how states and non-state actors use cyberspace to spread false information, manipulate public opinion, and destabilize societies. Case studies of Russian influence operations in the US and Europe, as well as Iranian and Hamas-led fake news in Israel, provide concrete examples of how mis/disinformation campaigns can influence political outcomes and erode trust in democratic institutions. He is right to ask questions with difficult answers like: how can a country retaliate over a fake story online? Is a fake story more dangerous to a nation than a missile? He argues that countries are not immune to

disinformation, which can destabilize and create chaos. Every nation decides how to retaliate over "fake news" while considering the risks of such retaliation.

Countries with robust cyber defense and controlled digital spaces – Secure Cyber Domains (SCD) – are explored in Chapter 6. Topor makes a structured and equal review of SCDs in North Korea, China, Russia, Iran, and Saudi Arabia. He also discusses internet shutdowns in India and Myanmar, among others. In contrast, Chapter 7 focuses on Vulnerable Cyber Domains (VCD), highlighting countries with more open and vulnerable internet spaces. He reviews the cyberspaces of the United States, the United Kingdom, and Israel. Topor also reviews European Cyberspace as a whole, to which he refers as a "cyber bloc" due to Europe's regulatory efforts aimed at governing cyberspace, such as the European Union's General Data Protection Regulation (GDPR), Digital Services Act (DSA), and Digital Markets Act (DMA), and others.

These frameworks in Chapters 6 and 7 represent attempts to balance national sovereignty with the need for international standards and cooperation. These chapters show critical differences in cyber sovereignty. The comparative analysis of secure and vulnerable cyber domains is among the book's strengths, offering insightful perspectives on how different nations strategize their digital governance. These chapters are instrumental in illustrating the practical manifestations of cyber sovereignty. Nonetheless, a more critical examination of the impact on civil society and international cooperation would have enhanced the analysis.

Topor explains that the book deals with strategy and not human rights. Yet, these strategies have far-reaching implications for us all. Restricting the internet, censorship, and limiting free speech can undermine fundamental human rights like freedom of expression and access to information, weakening democracy and civil society. These measures may stifle innovation, suppress dissent, and can lead to societal polarization, economic stagnation, and diminished global collaboration on human rights. A delicate line divides between too much censorship and not enough of it.

The book argues that while these efforts are a step in the right direction, achieving global consensus on cyberspace governance remains a formidable challenge. Finally, Chapter 8 presents Topor's predictions for the internet's future, discussing potential scenarios. Topor predicts four scenarios for the future development, or segmentation, of the internet: (1) the *Status Quo* of current affairs regarding cyberspace, (2) the emergence of applicable international law regarding cyberspace, (3) the creation of sovereign and secure "standalone" cyber domains, and (4) the formation of cyber blocs, exemplified by the evolving European cyberspace. While intriguing, these speculations sometimes feel overly deterministic, underestimating the potential for emergent technologies and civil society movements to reshape the digital landscape.

While the book provides a thorough analysis of state-centric perspectives on cyber sovereignty, it tends to overlook the implications for human rights and digital inclusion. The emphasis on national security and control may overshadow the importance of ensuring that cyberspace remains an open and inclusive platform for all users. A more balanced discussion of these issues would have strengthened the book's overall argument. Additionally, while the book acknowledges the role of non-state actors such as cybercriminals and terrorist organizations, it does not explore their impact in sufficient depth. These actors play a significant role in the digital landscape, and their activities can have profound implications for national security and international stability. One of the book's key strengths is its comprehensive and multidimensional analysis of cyber sovereignty. Topor successfully integrates historical, technical, political, and legal perspectives to provide a holistic understanding of the topic. This interdisciplinary approach makes the book a valuable resource for scholars and practitioners in international relations, cybersecurity, and digital governance. The use of in-depth case studies is another notable strength, providing concrete evidence to support Topor's arguments. *Cyber Sovereignty* makes a significant contribution to the literature of international relations and also cyber policies, especially in its interdisciplinary approach to dissecting the intersections of technology, security, governance, and society. The book is a crucial addition to the discourse on international security and the future of the internet, challenging readers to reconsider the role of the digital realm in global politics. Future research should build on this foundation, diving deeper into the nuanced impacts of cyber sovereignty on global digital equity and freedom.

About the author:

Dr Pnina Shuker is an expert on strategy and national security issues, public opinion, social resilience, and information warfare. She is also a Lecturer at the University of Haifa, “Shalem” academic college, and the Academic College of Law and Science. She holds research fellowships at the Jerusalem Institute for Strategy and Security (JISS), the Haifa Laboratory for Religious Studies at the University of Haifa, and the Weidenfeld Center for Jewish Studies at the University of Sussex.