Global Power Shift

Lev Topor

Cyber Sovereignty

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

Springer

Global Power Shift

Ample empirical evidence points to recent power shifts in multiple areas of international relations taking place between industrialized countries and emerging powers, as well as between states and non-state actors. However, there is a dearth of theoretical interpretation and synthesis of these findings, and a growing need for coherent approaches to understand and measure the transformation. The central issues to be addressed include theoretical questions and empirical puzzles: How can studies of global power shift and the rise of 'emerging powers' benefit from existing theories, and which alternative aspects and theoretical approaches might be suitable? How can the meanings, perceptions, dynamics, and consequences of global power shift be determined and assessed? This edited series will include highly innovative research on these topics. It aims to bring together scholars from all major world regions as well as different disciplines, including political science, economics and human geography. The overall aim is to discuss and possibly blend their different approaches and provide new frameworks for understanding global affairs and the governance of global power shifts.

All titles in this series are peer-reviewed.

This book series is indexed in Scopus.

Lev Topor

Cyber Sovereignty

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

Springer

Lev Topor
ISGAP-Woolf Institute
Cambridge, UK

ISSN 2198-7343 ISSN 2198-7351 (electronic)
Global Power Shift
ISBN 978-3-031-58198-4 ISBN 978-3-031-58199-1 (eBook)
https://doi.org/10.1007/978-3-031-58199-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

To Funny Cat Videos online. May this content never be blocked.

Preface

Within the span of a generation, the world has experienced a seismic shift caused not by tectonic plates but by cables connecting computers and running lines of code and project information to us all. The internet, once a hopeful utopia of boundless connection, has transformed into a turbulent digital archipelago. Countries (nation-states), no longer confined by physical borders, are staking a claim to their own sovereign cyberspaces by erecting firewalls and digital borders or disconnecting themselves from the global grid altogether through sheer tenacity. This book plots a daring course through this fragmented landscape, charting the treacherous shoals of national regulation, restricted access and the ever-present threat of complete disconnection.

The beginning of the twenty-first century has witnessed an unprecedented surge in the importance of cyberspace as a crucial arena for economic, political and social interaction. The internet, once heralded as a harbinger of global unity, now finds itself at a crossroads. The utopian vision of a borderless network, a free-flowing exchange of ideas and information, is increasingly under siege. From North Korea's Kwangmyong internet to the Great Firewall of China to Iran's Shabake-ye Melli-ye Ettelā'āt (National Information Network) to Russia's RuNet project and even the European Union's regulatory struggle for individual privacy, countries are crafting their own bespoke versions of the online world, often at the expense of open access and free speech. This book meticulously dissects these diverse cyber domains, revealing the unique challenges and motivations that drive each nation's digital agenda. One thing is clear: they are not afraid to compete with the Western dominance over the web.

This shift towards "cyber sovereignty" is not merely a technical phenomenon; it represents a fundamental reassessment of power and control in the twenty-first century. Information, once the lifeblood of democratic societies, is now wielded as a tool of both empowerment and repression. Information is now mis/disinformation. Governments, concerned about national security, social stability, and the erosion of cultural identities, are increasingly turning to digital gatekeeping to safeguard their interests. However, this comes at a steep price. As the book eloquently argues, the

fragmentation of the internet into siloed cyber spaces risks severing the very communication arteries that facilitate global dialogue, economic exchange and scientific collaboration.

The consequences of this fragmentation are far-reaching and multifaceted. The book outlines the impact on matters like human rights and free speech, global trade and scientific progress. The silencing of dissident voices within national firewalls, the chilling effects of self-censorship, and the potential for a "digital balkanization" are just some of the possibilities that loom on the horizon. The fight for a global internet, one that respects national sovereignty while upholding fundamental human rights, remains a complex and ongoing struggle. This book serves as a crucial roadmap for navigating this contested terrain, offering nuanced analyses of potential solutions and frameworks for international cooperation in the case of Secure Cyber Domains and cyber blocs.

But beyond the policy prescriptions and technical frameworks, this book also delves into the deeper philosophical questions that underpin the very notion of cyber sovereignty. It grapples with the tension between individual autonomy and national security, the delicate balance between free speech and societal cohesion, and the challenges of reconciling cultural diversity with a globalized digital realm. These are not merely technical problems to be solved but profound ethical dilemmas that demand careful consideration and ongoing dialogue. This book is a clarion call for a future where the internet can connect but respect. It is a call for a digital world that respects national sovereignty while fostering global connection, a world where the free flow of information empowers individuals and strengthens societies, and where the vast potential of the internet is harnessed for the betterment of all, not the abuse of all. As we embark on this digital odyssey, this book serves as a vital compass, guiding us through the uncharted binary waters of cyber sovereignty and towards a future where the internet remains a beacon of connection, not a weapon of division.

Cambridge, UK Lev Topor

Acknowledgements I would like to express my sincere gratitude to the following individuals and organizations who have contributed to the completion of this book: Prof. Arie Kacowicz, who advised on an early draft paper on the topic of cyber blocs presented at the Israeli Association for International Studies, Prof. Eldar Haber, with whom I have published a paper on the topic of sovereign cyber domains (which we referred to as "internet bubbles"), Dr. Alexander Tabachnik, who contributed his great insight on the Russian cyber domain, and the Center for Cyber Law and Policy at the University of Haifa, Israel.

Contents

Abbreviations

AI	Artificial Intelligence
APNIC	Asia Pacific Network Information Centre
APT	Advanced Persistent Threat
AR	Augmented Reality
ARPANET	Advanced Research Projects Agency Network
BIS	Bureau of Industry and Security
BRI	Belt and Road Initiative
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCP	Chinese Communist Party
CCPA	California Consumer Privacy Act
ccTLDs	Country Code Top-Level Domains
CDA	Communications Decency Act
CDN	Content Delivery Network
CERT-EU	Computer Emergency Response Team for the EU
CIS	Commonwealth of Independent States (former Soviet countries)
CISA	Cybersecurity and Infrastructure Security Agency
CISA	Cybersecurity Information Sharing Act
CNNIC	China Internet Network Information Center
CSIS	Center for Strategic and International Studies
CSO	Civil Society Organization
CST	Communications, Space and Information Technology Commission
DARPA	Defense Advanced Research Projects Agency
DIME	Diplomatic, Information, Military and Economic
DMA	Digital Markets Act
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DSA	Digital Services Act
ECJ	European Court of Justice
EIF	European Internet Forum
ENISA	European Union Agency for Cybersecurity

FCC	Federal Communications Commission
GCHQ	Government Communications Headquarters
GCI	Global Cybersecurity Index
GCSC	Global Commission on the Stability of Cyberspace
GDPR	General Data Protection Regulation
GEC	Global Engagement Center
GFW	Great Firewall
GGE	Group of Governmental Experts
GSP	Golden Shield Project
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IDF	Israel Defense Force
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IIX	Israeli Internet Exchange
INCD	Israel National Cyber Directorate
IoT	Internet of Things
IP	Internet Protocol
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
IUCC	Israeli inter-University Computation Center
IXP	Internet Exchange Point
MAD	Mutual Assured Destruction
NATO	North Atlantic Treaty Organization
NCA	National Cybersecurity Authority
NCC	National Center for Cyberspace
NCP	Network Control Protocol
NCSC	National Cyber Security Centre
NHS	National Health Service
NIC	Network Information Center
NIN	National Information Network
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NSC	National Security Council
NTIA	National Telecommunications and Information Administration
OEWG	Open-Ended Working Group
OFCOM	Office of Communications

OGAS	National Automated System for Computation and Information Processing (from Russian: ОГАС—Общегосударственная автоматизированная система учёта и обработки информации)
ONI	Open Net Initiative
OSA	Online Safety Act
OSI	Open System Interconnection
OT	Operational Technologies
PRC	People's Republic of China
PTI	Public Technical Identifiers
R2P	Responsibility to Protect
RIR	Regional Internet Registry
SATNET	Atlantic Ocean Packet Satellite Communications Network
SCC	Supreme Council of Cyberspace
SCD	Secure Cyber Domain
SMA	Secure Messaging Application
SORM	System of Operational-Investigatory Measures
TCP	Transmission Control Protocol
TLD	Top-Level Domain
UNGA	United Nations General Assembly
UPS	Uninterruptible Power Supply
US-CERT	United States Computer Emergency Readiness Team
VCD	Vulnerable Cyber Domain
VK	VKontakte
VR	Virtual Reality
W3C	World Wide Web Consortium
WEF	World Economic Forum

List of Figures

List of Tables

Chapter 1
Introduction

The internet, or cyberspace, refers to a virtual world of computers and "smart" devices that facilitate online communication and the transmission of information through interconnected digital environments. With the global population soon to reach 8 billion people (as of 2023), only approximately 2.6 billion of us are still offline. Approximately, 67%, or 5.4 billion people, are now using the internet. Regionally, 91% of Europeans are connected, 89% of the population of the Commonwealth of Independent States (CIS, former Soviet countries) is connected, 66% of the people in the Asia–Pacific region are connected, 69% of the population of Arab countries is connected, 87% of Americans (South, Central and North) are connected and 37% of Africans are connected. Most communication occurs via submarine fiber-optic cables and terrestrial cables (approximately 95%; some utilizes satellites). It seems like the whole world is being uploaded; since the internet has indeed become a form of mass communication—people are connected, organizations are connected and countries are connected—it has become a major proxy for international security.[1]

The cyber domain has emerged as the perfect platform for international influence and power struggles on the world stage. Now, not only global powers but also terror organizations, rogue lone-wolf terrorists and criminals execute their attacks in the cyber domain as well as in the real kinetic domain.[2] Just as Alfred T. Mahan observed in the late nineteenth century that "whoever rules the waves rules the world,"[3] it has become clear that whoever rules the cyber domain rules mass communications and, consequently, the world (or at least, a significant part of global affairs). In fact, the cyber domain can be considered a perfect platform for international influence not only because it enables global powers to virtually—but in a very real sense—invade and intervene in their adversaries with a few (very skilled) mouse clicks but also because, in the current state of affairs, there are no binding international laws and no clear

[1] See International Telecommunication Union (2023).

[2] See, generally, Lin and Zegart (2019).

[3] Mahan (2011).

L. Topor, *Cyber Sovereignty*, Global Power Shift,
https://doi.org/10.1007/978-3-031-58199-1_1

norms regarding cyberspace—every country can do what it considers appropriate. Successful attempts to agree upon such laws seem distant (i.e., the Tallinn Manual, the United Nations' GGE and OEWG),[4] although some legislative efforts such as the European General Data Protection Regulation (GDPR), Digital Services Act (DSA) and Digital Markets Act (DMA), as well as specific national legislations, do seem more likely to succeed.[5] Nevertheless, such regulations mainly concern blocs like Europe or sovereign nations such as Russia, China and a few others, not the entire world. Even in Europe, each nation has its own norms and regulations.

Meanwhile, under the present legislative conditions, cyberattacks and influence campaigns are perfectly legal. That is, the spread of malicious software, mis/disinformation campaigns, and leaks are not illegal. Cyberattacks that directly cause damage, human injuries or death may be retaliated against, but one has to forensically prove their source—an objective that is very difficult to achieve, as elaborated throughout this book. Since many cyber criminals utilize digital and real proxies, attribution is very difficult.[6] It is true that under the Charter of the United Nations, Chapter VII, Article 51, a country can take physical (kinetic) action against an armed attack, even an armed cyberattack; however, in its current structure, as Martin C. Libicki noted, cyberspace is tailor-made for strategic ambiguity.[7] Furthermore, the Twitter Revolution,[8] the Arab Spring,[9] and interventions in electoral and democratic processes by foreign actors, such as the United States presidential elections or cases like Brexit, have proven that even manipulated information in cyberspace can cause tremendous damage, often more than a kinetic attack.

Thus, what can nations do to protect themselves in this Wild West, in this lawless virtual domain? Since international relations and politics, in general, are reactionary, it is probable that countries will strive to control their cyberspaces and protect themselves.[10] As examples throughout this book make clear, countries like Russia and China are already taking action.

The main argument presented in this book, based on observation and formulated from a strategic point of view, is that because nations worldwide are currently striving to restrict their cyber domains in order to better control their domestic affairs and

[4] See Schmitt (2017); UN GGE—Group of Governmental Experts, UNGA Res. 73/266; UN OEWG—Open-ended Working Group, UN GA Res. 73/27.

[5] Digwatch (n.d.) and Shuker and Topor (2021).

[6] Harknett and Nye Jr. (2017).

[7] Libicki (2011). See United Nations (1945).

[8] The term "Twitter Revolution" has been used to refer to various revolutions and protests that utilized the social networking site Twitter as a communication tool. It has been associated with events such as the 2009 Moldova civil unrest, the 2009–2010 Iranian election protests, the political movements in Egypt during January and February 2011 and more.

[9] The Arab Spring refers to a series of anti-government protests, uprisings and armed rebellions that spread across the Arab world in the early 2010s. Social media, including Twitter, played a significant role in the Arab Spring by facilitating communication and interaction among activists, allowing them to organize demonstrations, disseminate information and raise global awareness of the events.

[10] See, generally, Lin and Zegart (2019).

better protect themselves from foreign cyberattacks and unwanted influences, we may, in the near future, see a different type of internet—a more restricted one. This, I call a Secure Cyber Domain (SCD). Simply put, an SCD is a border intended to preserve national sovereignty, specifically by controlling domestic mass communications and keeping out unwanted content of any kind. SCD is a flexible term that can be used to describe a country with a protected cyber domain, a standalone cyber domain or one shared with others (which I refer to as a cyber bloc), as long as it is secure and not (or less) susceptible to foreign influence and manipulation. In contrast, a Vulnerable Cyber Domain (VCD) is a domain that prioritizes freedom of information, whether true, false or harmful, over national resilience and public order.

Countries can manage to disconnect from globalization in this age of information just as they managed to halt certain aspects of globalization through lockdowns and border closures when the COVID-19 pandemic struck. In the case of the pandemic, nations eventually opened their borders to those tested for the virus and/or vaccinated against it. Closing cyber borders may be a bit more complex, but it is a very manageable task, as I demonstrate in subsequent chapters. Following on from this observation and argument, I also ask: How will the global internet be structured in future? Will processes of de-proliferation of connectivity undermine processes of globalization? How will such changes in mass communication affect human cooperation? How will this "digital balkanization" continue to develop?[11]

In a paper co-authored with Eldar Haber, these efforts to restrict the internet were referred to as "internet bubbles," meaning that a nation may create its own sovereign internet bubble—an enclosed national intranet.[12] Since writing that paper, I have developed this concept further as the international spread of mis/disinformation and cyberattacks has proliferated. Such sovereign cyberspaces, SCDs, might not only be constructed within nations but also within blocs and partnerships. Nations are taking advantage of the lack of regulations and legal frameworks to create such spheres. Nowadays, this is particularly true for Russia and China, which perceive the internet, a largely American project, as a domain that enables their global adversary—the United States—to maintain its power and global influence. In a world that is framed as tri-polar (or multipolar), Russian and Chinese concerns are not far-fetched; the United States has developed much of the global internet and controls its infrastructure either directly or via business proxies, high-tech companies, social media and secure messaging applications (SMAs).[13] Even the European Union, with the GDPR, DSA and DMA in place, has expressed concerns over American and corporate influence.[14]

It is important to note that the observations and arguments in this book focus on strategy, sovereignty and international relations and not on international human rights or debates on freedom of speech or freedom of information and truth—although the latter is touched upon. Furthermore, even though I personally lean toward the liberal

[11] Economist (2010).

[12] Haber and Topor (2023).

[13] Elkin-Koren and Haber (2016).

[14] For instance, the European Commission has challenged Meta (Facebook) over what in Europe are perceived as abusive practices. See European Commission (2022a) and Machangama (2022).

West, national sovereignty is of vast importance to the majority of nations in the world, even if they are less liberal and less democratic, and even if, personally, as a human but also as a researcher of politics and international affairs, I do not agree with them. In this book, I attempt to decouple from normative perspectives and focus on national strategy. Therefore, I explore how a country should act if it wants to either preserve or increase its sovereignty, considering the fact that countries—nations—generally seek to have greater sovereignty. The concept of sovereignty will be presented and explained in detail in Chap. 3, which deals with sovereignty, power and international security. The term sovereignty is, as the English historian Francis Harry Hinsley notes, complex but flexible:

> Men do not wield or submit to sovereignty. They wield or submit to authority or power. Authority and power are facts as old and ubiquitous as society itself; but they have not everywhere and at all times enjoyed the support or suffered the restraints which sovereignty, a theory or assumption about political power, seeks to construct for them. Although we talk of it loosely as something concrete which may be lost or acquired, eroded or increased, sovereignty is not a fact. It is a concept which men in certain circumstances have applied – a quality they have attributed or a claim they have counterposed – to the political power which they or other men were exercising.[15]

The situation is changing even as these lines are being written. Russia continues to develop its cyber sovereignty through its so-called RuNet project and is developing strict regulations against unwanted influences, including the Yarovaya law and the "sovereign internet" law. Russia also requires that a specific application be installed on new smartphones and other smart devices.[16] China continues its regulation and restriction of foreign platforms using its "Great Firewall"; Google, Apple, Meta (Facebook) and other American-based tech giants are not welcome in the People's Republic of China.[17] China also plans to rival the private American Starlink venture in space and launch its own constellation of satellites.[18] Furthermore, China is pursuing independence from the American-backed internet infrastructure as it works to rival, and presumably replace, American-backed undersea fiber-optic cables.[19] North Korea controls its own communication systems with the Kwangmyong intranet, which is entirely separate from the global grid.[20] Furthermore, even within the United States, private business entities are attempting to create restricted and sovereign business zones (i.e., "Innovation Zones" in Nevada), chipping away at American sovereignty.[21]

What motives have led countries to restrict their internet? The internet as we know it today is a largely American project. It was developed by American and Western defense and research entities and projects like the Advanced Research Projects

[15] Hinsley (1986: 1).

[16] Topor and Tabachnik (2021) and Wang (2020).

[17] Chandel et al. (2019).

[18] Cadell (2023).

[19] Brock (2023).

[20] Warf (2015).

[21] Metz (2021).