Democratization and Autocratization Studies

Authoritarian Actors and Strategic Digital Information Operations

The New Age of Manipulation

Edited by Ihsan Yilmaz
and Shahram Akbarzadeh

ROUTLEDGE

AUTHORITARIAN ACTORS AND STRATEGIC DIGITAL INFORMATION OPERATIONS

This book explores the complex web of Strategic Digital Information Operations (SDIOs) – defined as deliberate efforts by state and non-state actors to manipulate public opinion and emotions using digital technologies – that intersect with political ambitions to create a complex environment ripe for manipulation.

Drawing from extensive research and case studies, the book examines how actors ranging from authoritarian regimes to extremist groups such as ISIS, and even political entities in democratic countries, leverage digital platforms to further their agendas. As such, it provides a comprehensive overview of SDIOs, their evolving tactics, and implications for democracy, governance, and international relations. It examines the diverse tactics employed by these actors, from spreading half-truths and distractions to leveraging historical and religious narratives in the form of conspiracy theories or non-conspiracy narratives, aiming to control the discourse and shape the online environment to their advantage. This research challenges the conventional focus on disinformation, highlighting the shift toward more sophisticated and less discernible means of digital manipulation globally, and argues that SDIOs have become a pivotal tool for influencing public opinion, shaping political narratives, and even undermining democratic processes.

This book will be of key interest to scholars, students, and practitioners in communications/media studies, political sociology, comparative politics, security studies, political science, and international politics.

Ihsan Yilmaz is Deputy Director (Research Development) at the Deakin Institute for Citizenship and Globalization, Research Professor of Politics and International Affairs, and Chair in Islamic Studies at Deakin University, Australia.

Shahram Akbarzadeh is Director of the Middle East Studies Forum (MESF) and Professor of Middle East Politics at Deakin University, Australia.

Democratization and Autocratization Studies

Series Editors: Luca Tomini, *CEVIPOL, Université libre de Bruxelles, Belgium*, *and* Seraphine F. Maerz, *University of Melbourne, Australia*

This series offers a space to those interested in recent regime transition and transformation processes globally, both empirically and theoretically. It considers sole- or jointly-authored, and edited, volumes, both full length and shorter, as well as handbooks.

Democracies in Peril?
Waves of Backsliding
Hans Keman

Why Neo-Militant Democracies Endure
The Inner Six in Comparative Perspective
Joanna Rak

The Global Rise of Autocracy
Its Threat to a Sustainable Future
Edited by Barbara Wejnert

Quality of Democracy at Regional Level in the V4 Countries
Patterns and Institutions
Pavel Maškarinec

Authoritarian Actors and Strategic Digital Information Operations
The New Age of Manipulation
Edited by Ihsan Yilmaz and Shahram Akbarzadeh

For more information about this series, please visit: www.routledge.com/

AUTHORITARIAN ACTORS AND STRATEGIC DIGITAL INFORMATION OPERATIONS

The New Age of Manipulation

Edited by Ihsan Yilmaz and Shahram Akbarzadeh

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Designed cover image: © Getty Images

First published 2026
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

© 2026 selection and editorial matter, Ihsan Yilmaz and Shahram Akbarzadeh; individual chapters, the contributors

The right of Ihsan Yilmaz and Shahram Akbarzadeh to be identified as the authors of the editorial material, and of the authors for their individual chapters, has been asserted in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

For Product Safety Concerns and Information please contact our EU representative GPSR@taylorandfrancis.com. Taylor & Francis Verlag GmbH, Kaufingerstraße 24, 80331 München, Germany.

The Open Access version of this book, available at www.taylorfrancis.com, has been made available under a Creative Commons Attribution-Non Commercial-No Derivatives (CC-BY-NC-ND) 4.0 International license.

Any third party material in this book is not included in the OA Creative Commons license, unless indicated otherwise in a credit line to the material. Please direct any permissions enquiries to the original rightsholder.

The electronic version of this book was funded to publish Open Access through Taylor & Francis' Pledge to Open, a collaborative funding open access books initiative. The full list of pledging institutions can be found on the Taylor & Francis Pledge to Open webpage.

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-041-04370-6 (hbk)
ISBN: 978-1-041-04367-6 (pbk)
ISBN: 978-1-003-62808-8 (ebk)

DOI: 10.4324/9781003628088

Typeset in Sabon
by Apex CoVantage, LLC

CONTENTS

List of Illustrations *viii*
Notes on Contributors *x*
Acknowledgments *xx*

1 Goals, Practices, and Impacts of Strategic Digital Information Operations 1
Ihsan Yilmaz and Shahram Akbarzadeh

PART 1
Elections **23**

2 A Comparative Analysis of Pakistan's Digital Parties: Beyond Traditional Politics 25
Ramsha Jahangir

3 Dis/Misinformation, Visibility Politics, Populism, and Digital Information: An Analysis of Pre- and Post-2023 Nigerian General Elections 45
Najimdeen Ayoola Bakare

PART 2
Conspiracy Theories **63**

4 The Persistence of Informational Manipulation and the Appropriation of Emerging Events: Conspiratorial Publics 65
Katherine M. FitzGerald, Daniel Whelan-Shamy, and Timothy Graham

5 The Role of Social Media in the Diffusion of Conspiracy Theories and the Consolidation of Digital Authoritarianism in the Middle East: The Case of Egypt 86
Ihsan Yilmaz, Ali Mamouri, and Shahram Akbarzadeh

PART 3
Digital Authoritarianism **105**

6 #Propaganda: Manufacturing Consent through State Actors' SDIOs in Thailand 107
Itsakul Unahakate

7 Turkish Government's Domestic Digital Information Operations on X (Twitter), Democracy, and Social Cohesion 124
Ihsan Yilmaz, Bulent Kenes, and Nicholas Morieson

8 India's Strategic Digital Information Operations 141
Ihsan Yilmaz and Chloe Smith

9 Media as a Tool for Strengthening Authoritarian and Populist Tendencies in Central European Countries: A Case Study of Hungary 159
Martin Solik and Jan Graf

PART 4
Transnational Dynamics **175**

10 Iranian State-Sponsored Disinformation Against the Dissidents at Home and in the Diaspora 177
Shahram Akbarzadeh, Amin Naeni, Galib Bashirov, and Ihsan Yilmaz

11 The Influence of the Kremlin in the Media Space of Western Balkan Countries: A Case Study of Serbia 193
Jan Graf and Martin Solik

12 The Transnationalisation of Strategic Digital Information Operations: Turkey and India 209
Ihsan Yilmaz, Priya Chacko, Susan de Groot Heupner, and Anand Sreekumar

PART 5
Non-State Actors and Extremism 235

13 Differences in the Utilisation of Digital Tools for Information Operations Between State and Non-State Actors 237
Mohamed Ibrahim

14 Alt-Right Ideology, Masculinity, and the Strategy of Information Operations: Understanding Digital Dissonance 254
Aiden Aylett, Toija Cinque, and Jodi McAlister

15 Future Directions in Strategic Digital Information Operations and Warfare 278
Ihsan Yilmaz

Index 290

ILLUSTRATIONS

Figures

2.1 The proportion of posts about each topic is shown for each type of political actor within PTI and PML-N. 33

2.2 Semantic similarity per day in the month leading up to the election. 35

2.3 Plot showing the proportion of posts belonging to coordinated campaigns that relate to each of the topics from the previous section for PTI's coordinated campaigns and PML-N's coordinated campaigns, respectively. 37

2.4 (a, c) Histograms indicating the proportion of actors involved in coordinated campaigns for PTI and PML-N, respectively. (b, d) Histograms showing the proportion of earliest posts in a coordinated campaign for each actor for PTI and PML-N, respectively. 38

4.1 Visualisation of the volume of the post volume per hour for posts containing #MauiPsyOps. 78

4.2 Visualisation of the hashtags being utilised most frequently in conjunction with #MauiPsyOps. 79

14.1 *The Alex Jones Show* Word Cloud. 261

14.2 *Tate on Being the Best* Word Cloud. 264

14.3 *Tate on Hollywood & Masculinity* Word Cloud. 265

14.4 *Tate on Men Paying for Dates* Word Cloud. 265

14.5 *The Ben Shapiro Show* Word Cloud. 267

Tables

2.1 Designation, username, number of tweets, and mean engagement metrics for the ten core accounts. 32

Boxes

4.1 The post from @UserM shared by @WellnessInfluencer about aid reaching Maui. It has been anonymised due to the low account size of @UserM. 76
4.2 The first tweet containing the #MauiPsyOps hashtag. 77

NOTES ON CONTRIBUTORS

Editors

Ihsan Yilmaz is Deputy Director (Research Development), Deakin Institute for Citizenship and Globalization, Deakin University, Melbourne, Australia; Research Professor of Politics and International Affairs; and Chair in Islamic Studies. He is also Non-Resident Senior Fellow at Oxford University's Regent College and the European Center for Populism Studies, Brussels. He co-leads the Gerda Henkel Foundation (Germany) project with Professor Shahram Akbarzadeh titled: "Smart Digital Technologies and the Future of Democracy in the Muslim World" (2022–2025). He also leads two ARC Discovery Projects: "Civilizationist Mobilization, Digital Technologies, and Social Cohesion: The Case of Turkish & Indian Diasporas in Australia" (2022–2025) and "Religious Populism, Emotions, and Political Mobilization: Civilizationism in Turkey, Indonesia, and Pakistan" (2023–2026).

Shahram Akbarzadeh is Director of the Middle East Studies Forum (MESF) and Professor of Middle East Politics, Deakin University (Australia). He co-leads the Gerda Henkel Foundation (Germany) project "Smart Digital Technologies and the Future of Democracy in the Muslim World" (2022–2025) with Professor Ihsan Yilmaz. He held a prestigious ARC Future Fellowship on the Role of Islam in Iran's Foreign Policy-making and recently completed a Qatar Foundation project on Sectarianism in the Middle East. Professor Akbarzadeh has an extensive publication record and has contributed to the public debate on the political processes in the Middle East, regional rivalry and Islamic militancy. In 2023, he joined the Middle East Council on Global Affairs (Doha) as a Non-Resident Senior Fellow.

Chapter Contributors

Aiden Aylett is a PhD candidate with full scholarship at Deakin University, specialising in the study of digital creative writing communities. His current research centers on communal world-building and writing processes, particularly how digital platforms facilitate user collaboration. He interrogates the entanglement of technology, community, and creative practice in an online collaborative writing project titled "The SCP Wiki" to determine the potential contributions of these elements on the formation of genre. His research approach integrates both qualitative and quantitative methods to analyze the structure, functionality, and communication within digital communities. Previously, he focused on the communal production of genre in fanfiction communities for their Honours thesis, drawing on a combination of distant and close textual reading to analyze the roles of tagging conventions in genre communication, and the connections between source material and fanfiction genres. This topic was further extrapolated in a paper presented at the 2021 Independent Publishing Conference and formed the basis for an article now under review for a renowned Q1 Journal. Further research interests include genre studies, paratextual analysis, collaborative practices (particularly in the context of writing and world-building), cultural and social dynamics in digital communities, and gender and sexuality studies.

Najimdeen Ayoola Bakare is affiliated with the Department of International Relations and Strategic Studies, Faculty of Arts and Social Sciences, Universiti Malaya, Malaysia. His principal areas of interest are EU politics, Global politics, African politics, Issues of European Muslims, Regionalism, Developmental studies, Theories of IR, Minority issues, and (Islamic and Western) Philosophy. In addition to having almost two decades of teaching experience, he has also published reasonably on many issues in different international and local journals and books, which include *Contemporary African Studies*, *Journal of Asian and African Studies*, *Journal of Asian Security and International Affairs, Strategic Studies, Migration Studies*, *Journals of European Studies, IPRI Journal, Przeglad Strategiczny, Policy Perspectives, NUST Journal of International Peace & Stability, Routledge, Springer,* and *Rowman & Littlefield*, among others. He recently published the book *Arab-Israel Normalization: Global Perspective*.

Galib Bashirov was previously an associate research fellow at the Deakin Institute for Citizenship and Globalization, Deakin University, Australia. He is currently Specialist, Research Funding (Business and Law), Deakin University, Faculty of Business and Law, Research Services. His research examines state–society relations and the impact of digital technologies on political processes in the Middle East and Central Asia. His previous works have been

published in *Review of International Political Economy*, *Democratization*, and *Economy & Society*.

Priya Chacko is Head of the Department of Politics and International Relations at the University of Adelaide. Her current research focuses on the political economy of authoritarian populism in India, India's transnational repression and legitimation strategies. She is Chief Investigator with Ihsan Yilmaz on an ARC Discovery Project on "Digital Technologies and Social Cohesion: The Case of Turkish & Indian Diasporas in Australia" (2022–2025). She is Editor-in-Chief of the journal *South Asia: Journal of South Asian Studies*.

Toija Cinque is Associate Professor of Communications (Digital Media) at Deakin University. She founded the Intelligent Media Lab and leads the Critical Digital Infrastructures and Interfaces (CDII) research group. She draws on a broad scope of theoretical and methodological approaches, with projects using emerging screens and digital technologies for educational effect and change. Her research explores the challenges and opportunities of digital life. Her work examines the media developments of digitisation, datafication, and platformisation, focusing on the techno-cultural and environmental implications of data driven and algorithmically steered infrastructures and interfaces. She co-produced *Memories That Make Us: Stories of post World War 2 Italian migration to Australia*, a feature documentary that won Best Ethnographic Film in the New York International Film Awards and was Official Selection in the Asti International Film Festival, Italy; and Fiorenzo Serra Film Festival, Italy. Her publications include *Emerging Digital Media Ecologies: The Concept of Medialogy* (Routledge, 2025); *Changing Media Landscapes: Visual Networking* (2015); *The Dark Social: Online Practices of Resistance, Motility and Power* (co-edited, Routledge, 2023); *Materializing Digital Futures: Touch, Movement, Sound and Vision* (co-edited, 2022); and *Communication, Digital Media and Everyday Life* (co-written, 2015).

Katherine M. FitzGerald is a PhD candidate at the Digital Media Research Centre at the Queensland University of Technology (QUT). She has an academic background in psychology and digital communications. She uses qualitative and digital ethnography methods to study conspiracy theories, information disorder, and knowledge production on digital platforms. She supplements these methods with large-scale social media data analysis, providing a holistic perspective on the formation of conspiratorial beliefs. Her thesis focuses on exploring the dynamics of participatory knowledge production on online platforms. She has a particular interest in how the process of belief formation differs between conspiracy theorists and other forms of knowledge, and differences in social media user practices. She has published in journals such as the *Harvard Kennedy School Misinformation Review* and

Media International Australia. She has contributed her expertise to multiple edited volumes along, domestic and international media outlets, and Australian government policy submissions. In 2023, she received a Queensland University of Technology "Research and Innovation" Faculty Award and in 2024 received a Queensland University of Technology "Contribution to Public Policy and Debate" Faculty Award.

Jan Graf is currently a PhD student at the Department of Human Geography and Regional Development at the University of Ostrava. His research focuses on hybrid threats, Russian and Chinese geopolitics, and last but not least on the relations between the Western Balkan countries and the European Union. In the last four years, he has participated in several student grant competitions, which allowed him to engage in field research not only in the countries of the Western Balkans but also in Moldova. In 2021, he participated in field research in Bosnia and Herzegovina and Serbia, which resulted in two research studies. He also presented the results of his research several times at international conferences (Skopje, Banska Bystrica). In the summer of 2023, he participated in another field research in Montenegro, where he mapped the influence of the Russian Orthodox Church on Montenegrin society. Last year, he managed to collect primary data in Belgrade on the Kremlin's hybrid operations in the Western Balkan country. These data serve two purposes: First, to complete the dissertation that he is working on, and second, to write a comprehensive study that will attempt to map the most important features of Russian hybrid threats in Serbia.

Timothy Graham is Associate Professor of Digital Media at the Queensland University of Technology (QUT). His research interests explore the relationship between technology, truth, and knowledge, with a particular focus on propaganda, digital publics, and algorithmic curation. He is Australian Research Council DECRA Fellow, for his project, "Combatting Coordinated Inauthentic Behaviour on Social Media" (2022–2025). He is also Chief Investigator of the QUT Digital Media Research Centre and Associate Investigator of the ARC Centre of Excellence in Automated Decision-Making and Society (ADM+S). In 2024, along with colleagues he commenced a new ARC Discovery Project, "Understanding and Combatting 'Dark Political Communication'" (2024–2027). He has authored over 40 peer-reviewed journal articles and book chapters, featured in thousands of news articles in leading outlets including *The New York Times*, *The Guardian*, *ABC News*, *The Washington Post*, and *BBC World News*, and develops open-source software for the collection and analysis of data from the web and social media.

Susan de Groot Heupner is a political sociologist with a research focus on populist mobilisations and the formation of hegemonic ideological constructions.

She is Adjunct Fellow at the Griffith Centre for Social and Cultural Research and Associate Research Fellow at the Deakin Institute for Citizenship and Globalization. She works on two Australian Research Council projects examining religious populism, transnational polarisation, and emotive mobilisation. Furthermore, she is coordinating a national survey on Indigenous media in Australia. She is Managing Editor for the *Journal of Alternative and Community Media* and Editorial Board member for the Political Sociology section at *Sociology Compass*. She has published in journals such as *Politics and Religion*, *Religions*, *Journal of Intercultural Studies*, and *Journal of International Communication*, and has a forthcoming monograph with Leiden University Press. She has also contributed to public media platforms like *The Conversation, ABC*, and *Enlighten*.

Mohamed Ibrahim is former Somali Telecommunication Minister and now Fellow Researcher at Swinburne University and involved in community-related activities with Melbourne University. He is focused on researching the role of Fintech in enhancing the national economies of developing countries. He has been in the IT industry for over the last 25 years before moving into academia. He has worked for organisations, including Papua New Guinea's Electricity Commission (Elcom) as an IT engineer, Kuwait Oil Company as a system analyst, and United Arab Emirates Higher Colleges of Technology as a researcher, lecturer, and ICT consultant. He has been an honorary senior lecturer at Monash University, ICT strategy Director at Deakin University, and Chief Information Officer at Peninsula, where he was responsible for delivering technical strategies focusing on their social and community impacts. He was Founder of the Somali ISOC Chapter, which promotes internet access in Somalia. He was also Chairman of the Centre for Research and Dialogue during 2010–2014 and Somalia's Internet Governance Forum (IGF) representative. He participates actively and contributes to Internet Corporation for Assigned Names and Numbers (ICANN) conferences. He is involved in the ICANN country code names supporting organisation (ccNSO), the African Top-Level Domain Names (AfTLD), and ICANN Government Advisory Council (GAC) on behalf of Somalia, among other fora. Other ongoing current activities he is involved in are in the Fintech industry, Yeel, iiKEEN, and iiSHEEG startups, which are online businesses that deliver remittance and online data storage and retrieval solutions for the Somali community in Australia and in the wider global diaspora. Somsog (somsog.org) is another of his initiatives, which is part of online education platforms targeting the Somali community to raise awareness of civics duties and secure ways of using online services.

Ramsha Jahangir is an award-winning Pakistani journalist and policy expert specialising in technology and human rights. She holds Joint Master's in

Journalism, Media, and Globalization from the University of Amsterdam and Aarhus University and was awarded the prestigious Erasmus Mundus Journalism scholarship. For her Master's dissertation, she analyzed the populist communication style of Pakistani leader Imran Khan on Twitter (now X) during his tenure as prime minister. Over the past decade, she has extensively reported on internet censorship, surveillance, digital politics, disinformation, and the influence of tech platforms. Previously, she was a reporter for *Dawn*, Pakistan's leading English newspaper, and her investigative work has been featured in *Coda Story* and other international outlets. Currently, she is Associate Editor at *Tech Policy Press*, a nonprofit media outlet covering technology and democracy. Previously, she led policy and communications at the Global Network Initiative, and continues to contribute as Senior Fellow, addressing critical issues on human rights and technology. She is a regular speaker at events related to the internet and democracy, press freedom, and gender. She divides her time between Amsterdam and Karachi.

Bulent Kenes is an academic and journalist with over 25 years of professional experience. Besides his academic studies, he has managed multiple publications, in both Turkish and English. He has held top editorial positions at various media outlets such as *Zaman Daily*, *Turkish Daily News*, and *Anadolu*. He was editor-in-chief of *Bugün Daily* (2006) and founding editor-in-chief of *Today's Zaman* (2007–2016). He was among the founders of the Stockholm Center for Freedom. He served as voluntary chief editor from 2017 to 2019. He is based in Stockholm, where he lives as an exiled Turkish journalist and academic. He is also among the founders of the European Center for Populism Studies (ECPS). He received his BA in international relations and political science from Bosporus University, his MA from the Institute of Middle East Studies at Marmara University, and an MBA from now-closed Fatih University. He also received his PhD from Marmara University's Institute of Middle East Studies and wrote his dissertation on Iran's foreign policy after the 1979 revolution. At Fatih University, he lectured on international relations, the Middle East, political science, and media and communications. He has been a regular columnist and opinion writer for many publications, including *Turkish Daily News*, *Turkish Probe*, *Bugün*, *Zaman*, *Today's Zaman*, *The Guardian*, and *TR724*. He has also served as a TV host and commentator/debater on political shows. He has published six Turkish books and one English book on Iran, Turkish politics, human rights, and Islam's image. He is currently researching the impact of rising populism and authoritarianism across the globe. He, who is a member of the Swedish Union of Journalists (Journalistförbundet) and Swedish Publishers' Club (Publicistklubben), can speak Turkish (native), English, and Swedish.

Ali Mamouri is a scholar and journalist in the fields of philosophy and theology. He serves as Research Fellow at the Deakin Institute for Citizenship and Globalization at Deakin University. He has previously held positions as a lecturer at the University of Sydney (2014–2015), the University of Tehran (2008–2011), and Al-Mustansiriyah University (2009–2011). From 2020 to 2022, he served as a strategic communication advisor to the Iraqi prime minister, contributing to regional dialogue efforts between Iran and Saudi Arabia within Iraq. He also served as the editor of *Iraq Pulse* at *Al-Monitor* from 2016 to 2023, where he covered Iraq's political development during this crucial time. His work focuses on themes such as political Islam, secularism and religiosity, religious minorities, and interfaith dialogue. His writings and analyses have been featured in publications including *Al-Monitor*, *The Conversation*, the *Washington Institute*, *BBC Persian*, and *Al Jazeera*, *Friedrich Ebert Foundation*, among others.

Jodi McAlister is Senior Lecturer in Writing, Literature and Culture at Deakin University. Her work focuses on popular fiction and culture, with a particular interest in the role that emotions play in popular storytelling, and the affordances of different genres, structures, and media in facilitating emotional communication (including audio media). Her research combines traditional literary study methods with sociological and more experimental approaches, seeking to understand not just texts but the conditions in which they are produced. She is the author of three monographs – *The Consummate Virgin: Female Virginity Loss and Love in Anglophone Popular Literatures* (2020), *New Adult Fiction* (2021), and *Publishing Romance Fiction in the Philippines* (with Claire Parnell and Andrea Anne Trinidad, 2023) – with two more forthcoming: *The Bonkbuster: Women's Popular Reading in the Long 1980s* (with Amy Burge, 2026) and *Audio Erotica* (with Athena Bellas, Routledge, 2026). She has also written numerous book chapters and articles in journals such as *Continuum, Sexualities, Porn Studies, Celebrity Studies, Sexuality and Culture*, *Creative Industries Journal*, and *Media International Australia*. In addition, she is a novelist: her eighth novel will be published in June 2025.

Nicholas Morieson is Research Fellow at the Deakin Institute, Deakin University, Melbourne, Australia. He was previously a lecturer at the Australian Catholic University, Melbourne. He is the author of two books: *Religions and the Global Rise of Civilizational Populism*, and *Religion and the Populist Radical Right: Secular Christianism and Populism in Western Europe*, and many scholarly articles and commentaries on populism. He is an associate investigator on two Australian Research Council (ARC) Discovery projects: "Civilisationist Mobilisation, Digital Technologies, and Social Cohesion: The Case of Turkish & Indian Diasporas in Australia" and "Religious Populism,

Emotions, and Political Mobilisation: Civilisationism in Turkey, Indonesia, and Pakistan."

Amin Naeni is a PhD candidate and Research Assistant at the Deakin Institute for Citizenship and Globalization (ADI) at Deakin University, Australia. His research examines the relationship between digital technologies and socio-political developments in Iran, focusing on how authoritarian regimes leverage digital tools to control information, shape public discourse, and counter political dissent. His work also investigates the role of social media in identity politics, activism, and state-sponsored disinformation campaigns. Beyond Iran, his research interests extend to the resurgence of geopolitics in international relations, particularly in the context of revisionist powers and their challenge to the existing global order. He analyzes how these states use digital influence operations, cyber strategies, and media narratives to advance their geopolitical objectives. He is also Fellow at the Center for Middle East and Global Order (CMEG). His academic work has appeared in the *Journal of International Affairs*, *Contemporary Politics*, and *Middle East Policy*. He has also contributed to leading policy and media platforms, including the Middle East Institute, *The Conversation*, the *Brookings Institution*, and the *Atlantic Council*, among others. He earned his MA in Middle East and North Africa Studies from the University of Tehran in 2018.

Chloe Smith is a PhD candidate at the Deakin Institute for Citizenship and Globalisation at Deakin University, Australia. Her thesis studies religious populism and affective mobilisation in the cases of India and Indonesia. She is currently a research assistant in two ARC Discovery Projects: (1) "Civilisationist Mobilisation, Digital Technologies, and Social Cohesion: The Case of Turkish & Indian Diasporas in Australia" and (2) "Religious Populism, Emotions, and Political Mobilisation: Civilisationism in Turkey, Indonesia, and Pakistan." She holds a Master of Islamic Studies and a BA in Counter-terrorism, Security, and Intelligence. She completed an internship with the global counter-extremism and counterterrorism organisation Hedayah and has previously worked for the Islamophobia Register Australia.

Martin Solik, PhD, MPA, is Assistant Professor at the Department of Human Geography and Regional Development at Ostrava University in Czechia. He has a solid experience with field research in the post-Soviet and Balkan space. In his research, he focuses on political power, new forms of hybrid warfare and hybrid threats, right- and left-wing political extremism, and radicalism in Europe. At Ostrava University, he teaches courses related to international politics, international relations theory, new forms of hybrid warfare and hybrid threats, and the world power system. He has written several articles in Slovak, Czech, and English regarding political power and the issues of hybrid

threats and warfare. During the last four years, he has participated in several field trips in the Western Balkans and Moldova together with Jan Graf. These field trips have resulted in several papers in prestigious international journals and two conference papers. He is currently involved at the University of Ostrava, where he will be working on the issue of hybrid interference between Russia and China in different regions of the world. The results of the research will be presented at international conferences and in academic journals.

Anand Sreekumar is a PhD candidate at the Department of Politics and International Relations within the School of Social Sciences at the University of Adelaide. His PhD dissertation seeks to uncover a global history of the Kerala model, focusing on its interconnections with global structures and discourses. He holds an MPhil in diplomacy and disarmament from the Centre for International Politics, Organization and Disarmament (CIPOD) at the School of International Studies, Jawaharlal Nehru University (JNU). He also has an Integrated Masters in Development Studies from the Indian Institute of Technology Madras. His works have appeared in both global and local journals as well as books, including *International Affairs*, *European Journal of International Security*, *South Asia: Journal of South Asian Studies*, *World Scientific*, and *Economic and Political Weekly*, among others. He has also contributed to public platforms like *The Conversation* and *Verfassungsblog*. His research interests span South Asia, political economy, intellectual history, and nuclear issues. He also served as a research fellow at the International Institute of Migration and Development (IIMAD) and has worked on an ARC project on civilisationist mobilisation, digital technologies, and social cohesion.

Itsakul Unahakate is a PhD candidate at the Department of Political Economy, Faculty of Arts and Social Sciences at the University of Sydney. His research interests include the political economy of social media, particularly misinformation and disinformation. His thesis focuses on the state's responses to "fake news" in Thailand. He is also a lecturer at the Faculty of Economics, Thammasat University, Thailand, where he teaches political economy and institutional economics.

Daniel Whelan-Shamy is a PhD candidate at the Digital Media Research Centre. His work is focused primarily on the application of critical social theory to the study of Generative Artificial Intelligence (GenAI). Using Jean Baudrillard's work on simulation – a theory that views communication as being abstracted from its original human form through the presence of increasingly distinct technological logics – Dan's PhD research examines how GenAI functions as a "simulating machine" across its computational architecture, the

user interface, and at a wider level of political economy. Through the analysis of these three interconnected levels of GenAI, he argues that there is increasingly clear evidence that simulation is pursued by technology companies as a political project directed toward the goal of building artificial general intelligence – a technology that many Silicon Valley executives believe will usher in an era of technologically facilitated millenarianism. He is also a member of the ARC Centre of Excellence for Automated Decision-Making and Society (ADM+S) and is interested in the study of misinformation and disinformation, as well as the philosophy of technology. He speaks Chinese and is curious about the growing geopolitical importance of GenAI technologies.

ACKNOWLEDGMENTS

This work was supported by the *Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.*

1

GOALS, PRACTICES, AND IMPACTS OF STRATEGIC DIGITAL INFORMATION OPERATIONS

Ihsan Yilmaz and Shahram Akbarzadeh

Introduction

In an age defined by digital technologies and constant connectivity, the sociopolitical sphere has undergone a significant shift. Both state and non-state actors currently operate in an expanded and increasingly digital arena, using its platforms to shape opinion, steer emotion, and secure strategic advantage. The convergence of political ambition with digital tools that can facilitate manipulation and political influence has created a highly contested space where narratives are engineered, dissent is managed, and support is manufactured across local, national, transnational, and global contexts.

This book introduces Strategic Digital Information Operations (SDIOs) as a framework that accounts for the emotional, psychological, technological, and sociopolitical dimensions of contemporary information manipulation. Moving beyond the traditional focus on military and political information warfare, the SDIO concept captures how actors use digital ecosystems to evoke emotional reactions, distract from key issues, overwhelm information channels, and seed long-term ideological alignment. It also highlights how public perception, trust, and digital literacy are central to the impact and success of such efforts.

We define SDIOs as deliberate, technology-enabled campaigns by state or non-state actors that manipulate the information environment to influence public attitudes, perceptions, and affective responses (Yilmaz et al. 2023). These operations are not random; they are strategically designed to support the sociopolitical goals of those behind them. Unlike analog-era propaganda or misinformation, SDIOs use algorithmic amplification, artificial intelligence, machine learning, personalisation of messaging, and big data analytics

DOI: 10.4324/9781003628088-1
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

to reach audiences with unprecedented speed, scale, and precision. Examples of SDIOs span democratic and authoritarian settings. For example, in Egypt, Turkey, Iran, and Pakistan, these operations target independent media to silence dissent (Akbarzadeh et al. 2024a, 2024b, 2025; Ahmed et al. 2024). Non-state actors, including fringe and extremist groups like ISIS and Al-Qaeda, have also built sophisticated digital strategies to recruit supporters and spread propaganda (Ingram 2015; Theohary 2011).

While the term "Information Operations" (IO) has been used in relation to online platforms such as Facebook to describe mechanisms of sidelining dissent and promoting conformity (Starbird et al. 2019; Hatch 2019), following Yilmaz et al. (2023), we aim to refine and extend the concept in two important ways. First, we foreground the strategic intent – the case studies in this book describe politically motivated operations aimed at specific outcomes. Second, we emphasise the digital medium, which makes these operations fundamentally different from earlier forms of communication warfare and propaganda.

Manipulation strategies once reliant on limited print or broadcast dissemination now involve bot farms, deepfake videos, real-time sentiment analysis, and coordinated influence campaigns. SDIOs are used to steer public discourse, attack opponents, polarise communities, and manufacture consent. They are dedicated not only to controlling facts but also to manipulating emotions and collective meaning-making.

Importantly, SDIOs are not confined to national borders. As digital networks transcend geography, so too do these campaigns. Governments increasingly use SDIOs to influence foreign publics, mobilise diasporas, discredit critics abroad, and sway global opinion in their favor. Consequentially, SDIOs function as tools of both domestic governance and international influence.

This chapter introduces the concept of SDIOs and sets the foundation for the book's broader analysis. The chapters that follow are organised around five key themes: how SDIOs shape elections and voting behavior; the use of conspiracy theories to erode trust and manipulate beliefs; the strategies of digital authoritarianism used to suppress opposition; the transnational operations of states seeking to control diasporas and global narratives; and the methods employed by non-state actors, including extremist groups, in their digital campaigns.

Strategic Digital Information Operations

The use of information as a strategic weapon is not a recent development. Across different historical periods, states and sub-state actors have engaged in influence operations to advance their interests, manage public opinion, and shape ideological environments both within and beyond their borders

(Yilmaz & Shakil 2025; Yilmaz et al. 2025). From the propaganda disseminated through print publications in early nation-states to the psychological operations deployed during the Cold War, information has consistently been mobilised to construct realities, reinforce authority, and delegitimise adversaries. These campaigns often rely on the spread of falsehoods, half-truths, and manipulated data to erode trust, sow confusion, and produce uncertainty. The goal is not merely to deceive but to create fragmentation in public knowledge and understanding, and to disempower collective action by overwhelming and polarising audiences with contradictory narratives.

The disruptive impact of disinformation is particularly amplified during high-pressure, time-sensitive events such as elections, national emergencies, diplomatic conflicts, and natural disasters. In such moments, the demand for real-time updates and clarity about the event and its impacts leaves audiences vulnerable to emotional and cognitive manipulation. Disinformation thrives in this climate of urgency. The 2016 US presidential election is a widely cited example where both state and non-state actors weaponised digital platforms to undermine trust in the electoral system and influence voting behavior. Reports revealed that digital campaigns specifically targeted African American voters, with an estimated 3.5 million Black Americans discouraged from voting through misinformation campaigns orchestrated via Facebook (Sabbagh 2020). This illustrates how SDIOs are not only strategic but also demographically calibrated, exploiting racial and political divisions.

What distinguishes today's IO from historical practices is the scope and sophistication introduced by digital technology. The widespread availability and low cost of social media platforms have transformed the nature of information warfare, making it more accessible, scalable, and granular. Platforms such as Facebook, YouTube, Twitter/X, Instagram, and Telegram are no longer passive channels of communication – they are actively engineered environments where algorithms prioritise content that triggers emotional responses and prolonged engagement.

In environments where political elites discredit legacy media, public trust shifts toward social media, where audiences are less protected from manipulation. Populist leaders in particular benefit from these dynamics, as echo chambers reinforce their narratives and algorithmic bias elevates polarising content. These conditions have created fertile ground for digital authoritarianism and contributed to what scholars describe as a global shift toward more illiberal governance models.

Digital manipulation campaigns are not confined to authoritarian regimes. Democratic states have also adopted techniques to manage perceptions and exert influence. Studies have identified social media manipulation operations in both democratic and authoritarian contexts, often targeting both domestic and international audiences. These operations rely on a hybrid architecture of fake accounts, coordinated bot activity, and human-operated troll networks.

The mechanics of these campaigns involve highly coordinated digital labor. Troll armies and disinformation networks craft narratives, circulate memes, manipulate trending topics, and target opponents. Trolls may function independently or be organised under party-affiliated cells, often attacking journalists, academics, opposition politicians, and civil society figures. Bots, both malicious and benign, supplement these efforts by amplifying messages and simulating public consensus. Many of these networks are capable of operating across platforms, adapting content formats to maximise virality and evade detection.

Democracies do often respond to these threats, but they vary in their resilience and ability to respond to them. Northern European countries, with stronger public broadcasting systems and higher media literacy, appear more resistant to online disinformation, while Southern European states and the US are more susceptible. This vulnerability is exacerbated by structural features of liberal democracies, such as freedom of expression and a less centralised media environment. These features, while foundational to democratic governance, are increasingly exploited by authoritarian and non-state actors to undermine legitimacy and sow distrust.

In response to the attempts to regulate harmful content, the actors directing SDIOs have developed more subtle and technically advanced methods. These include encrypted disinformation via direct messaging apps, targeted ads embedded with emotionally manipulative imagery, and operations designed to distract rather than deceive its audiences (Yilmaz et al. 2023; Iwuoha 2020). Disinformation, for instance, does not always involve falsehoods. Even factual information can be used in misleading ways – stripped of context, re-sequenced, or selectively framed. To further illustrate this point, influence operations can be classified into three categories: constructive (which aim to establish coherent alternative narratives), disruptive (which seek to break down existing narratives), and distractive (which deflect attention by highlighting unrelated issues). Astroturfing, another frequent tactic, simulates grassroots support where none exists, further obscuring the line between organic public discourse and state-sponsored manipulation.

As users and platforms have become increasingly aware of and responsive to overt falsehoods, the tactics behind SDIOs have evolved. While the circulation of outright lies continues to form an important part of the arsenal, strategic actors have increasingly turned toward more subtle forms of manipulation, including the selective presentation of facts, the deployment of half-truths, and the flooding of digital spaces with distracting or irrelevant information (Iwuoha 2020). The sophistication of these operations had grown in direct response to platform moderation efforts by leading social media giants like Facebook, Twitter/X, and YouTube, while these platforms were effectively moderating the content until recently. As algorithms and moderation teams attempt to identify and reduce the reach of false and

misleading information, disinformation campaigns have adapted by embedding their messaging in more ambiguous, emotionally resonant content that is harder to detect and regulate.

Rather than relying exclusively on lies, actors now aim to create what might be described as "information noise." These operations overwhelm users not only with false information but also with redundant, off-topic, or low-value content. The goal is to exhaust the audience's capacity to discern relevance or truth, weakening their ability to meaningfully engage with pressing political issues. These campaigns employ trolls, bots, paid influencers, PR firms, and, crucially, everyday citizens who can become active or passive amplifiers of the messaging (Mir et al. 2022). A clear example of this is found in China's "positive energy" campaign, where the government employed thousands of influencers and troll accounts to drown out critical voices. In one case, Uyghur individuals were brought forward at state-managed press conferences to share scripted narratives, designed to discredit global human rights concerns and recast repression as a benevolent style of governance (Chen et al. 2021; Mason 2022).

This strategy of saturation and distraction is neither accidental nor peripheral – it is central to the evolving practices of SDIOs. It reveals how these operations function not merely by inserting false claims into the public discourse but by reshaping what that discourse consists of in the first place. In Egypt, for instance, even amid a severe economic crisis that left millions without stable electricity, the regime saturated the media with celebratory stories about Egypt's supposed surplus in energy production and its potential as an electricity exporter to Europe. This kind of deflection does not require outright lying but instead reorients public attention toward a carefully crafted and deceptive narrative (Dawoud 2023).

The architecture of manipulation is also shaped by the very fabric of digital platforms. Algorithms create "filter bubbles" and echo chambers, insulating users from dissenting viewpoints and reinforcing pre-existing biases. Online antagonism – trolling, flaming, and baiting – further distorts conversation, suppressing deliberation and driving polarisation. Trolls can be individual actors or part of broader infrastructures such as state-linked "troll factories".

Bots play a central role in these operations. They spread disinformation, spam networks, overwhelm servers through denial-of-service (DDoS) attacks, and propagate malware and scams. However, what makes them particularly dangerous is their ability to mimic human behavior. Bots come in various forms: hackers who infiltrate systems, spammers who flood networks with unwanted content, impersonators who hijack identities to spread disinformation, and sock puppets, which are fake personas used to manipulate discourse and create an illusion of collective support or outrage. These tools are especially potent when deployed in botnets – interconnected networks of bots that work in coordination to magnify reach and influence.

Also central to these practices is the deployment of strategic narratives. These narratives are designed with a deep understanding of the cognitive and emotional dispositions of their target audiences. They are not, therefore, random; they are tailored to align with pre-existing beliefs, collective memories, and cultural reference points (Bakir & McStay 2018; Yilmaz et al. 2025). In some cases, the success of these narratives relies less on the persuasiveness of their factual content and more on their capacity to trigger emotional or ideological resonance. For many users, particularly those embedded in partisan or ideological communities, confirmation bias becomes a key driver of engagement. Strategic narratives then function not merely to inform but to reinforce, polarise, and motivate their target audience.

Among the most potent narrative techniques employed in SDIOs are those that rely on historical grievances and religious identity. These frames evoke powerful affective responses and mobilise collective memory as a tool for political persuasion. Often used in digital authoritarian contexts, these stories integrate conspiracy theories and half-truths, often into a framework of divine mission and historical redemption, encouraging loyalty to the regime while demonising internal and external critics (Yilmaz & Shipoli 2022; Yilmaz & Albayrak 2021; Yilmaz & Demir 2023).

Importantly, SDIOs are not always the product of centrally coordinated campaigns. They often instead emerge through informal, distributed, and sometimes unintentional collaboration among human actors. Digital influence operations can gain strength from the participation of organic communities – users who may not be formally linked to state or organisational campaigns but who nonetheless become vectors for the spread of propaganda and disinformation. During the 2016 US elections, for example, Russian-linked accounts from the Internet Research Agency operated thousands of fake personas, some posing as progressive or conservative American activists. These accounts successfully infiltrated online communities, organised real-life protests, and collaborated with unsuspecting activists, thereby blurring the line between orchestrated disinformation and organic mobilisation (Walker 2017). This complexity makes SDIOs harder to detect and disrupt. Their power lies in their ability to co-opt real people (cognisant and not) into networks of manipulation, transforming influence operations into participatory endeavors.

Goals of Strategic Digital Information Operations

SDIOs are used to achieve political outcomes by shaping how populations think, feel, and act. These goals span domestic and international contexts, targeting citizens, political adversaries, diasporas, and foreign publics. At the national level, SDIOs often seek to control narratives about governance, national identity, and legitimacy. In authoritarian settings, such operations

are deployed to suppress dissent, marginalise independent journalism, and create a political environment where criticism of the state is equated with disloyalty. In the digital realm, authoritarian governments use a combination of emotional storytelling, fear-based propaganda, and moral framing to present themselves as guardians of stability and national values (Yilmaz et al. 2024). They construct enemies, both real and imagined, to deflect from economic and political failures.

In Egypt, for example, digital narratives have painted independent journalists and opposition candidates as foreign agents serving Western agendas. Conspiracy theories play a prominent role in discrediting opposition (Akbarzadeh et al. 2025). These narratives are designed to undermine the credibility of dissent while reinforcing the state's legitimacy as a bulwark against foreign intervention (Michaelson 2018). In China, the state deploys advanced data analytics and narrative management tools such as the iMedia platform, which monitors and guides public sentiment online, suppresses dissent, and promotes ideologically "positive" messaging.

Emotional manipulation is central to these efforts. Authoritarian governments routinely invoke fear, resentment, pride, and anger to fortify their authority. In some authoritarian settings, emotions such as humiliation, disgust, and rage are instrumentalised to justify the pivot away from democracy (Yilmaz 2021). Narratives of victimhood – often blaming foreign conspiracies or domestic enemies – are used to galvanise support, silence critics, and unify supporters behind a shared sense of grievance and purpose (Yilmaz 2021; Tokdoğan 2020; Yilmaz & Shipoli 2022). These tactics produce an emotionally charged climate where citizens are more likely to accept repression and surrender civil liberties in exchange for security and moral clarity. Over time, this cultivates a fractured public sphere and entrenches authoritarianism by weakening political opposition and pluralism.

While both state and non-state actors use SDIOs, their methods, resources, and objectives differ. States usually have superior technological infrastructure, access to digital surveillance tools, and institutional reach. Their campaigns are more likely to be long term, data driven, and operationalised across multiple agencies and platforms. These operations may involve international cyber strategies designed to influence foreign elections, destabilise adversaries, or project soft power abroad. Non-state actors – such as extremist groups, hacktivist collectives, and transnational advocacy organisations – often lack the same scale but operate with agility. They often adapt more rapidly to changing digital norms and platform policies, often exploiting gaps in regulation and moderation to spread their messages. Their goals may include recruitment, radicalisation, or the promotion of ideological alternatives to state authority.

Digital platforms are increasingly shaped by the political interests of those who can most effectively manipulate them. Authoritarian regimes use these

platforms for censorship, surveillance, and legitimacy-building. Populist leaders, on the other hand, use them to bypass traditional media, forge direct emotional bonds with followers, and frame themselves as the voice of the "real people" against corrupt elites (Perloff 2021). This populist strategy creates polarising political dynamics in which opposition is not merely contested but vilified. Online ecosystems are not solely sites of communication but become battlegrounds where misinformation, moral panic, and emotional appeals emerge as tools of governance (Postill 2018).

In this context, SDIOs are not simply media strategies. They are mechanisms of governance and control, affecting how people think about power, identity, and legitimacy. Their effects ripple far beyond the digital sphere, reshaping political culture and institutional accountability.

Theoretical Contributions of This Book

This book offers an in-depth investigation of SDIOs by situating them within the broader currents of global politics, sociotechnical change, and evolving authoritarian practices. In doing so, it moves beyond conventional analyses of cyberwarfare and IO, developing a framework that captures the technological, psychological, emotional, and sociopolitical dimensions of digital manipulation. By integrating empirical case studies with theoretical insights, the book addresses long-standing gaps in scholarship across the fields of political communication, digital authoritarianism, international security, and media studies.

A central contribution of this volume is its comprehensive exploration of how SDIOs are deployed by both state and non-state actors in pursuit of political, ideological, and strategic goals. It traces the proliferation of these operations across a wide range of settings, from highly authoritarian regimes to formally democratic polities exhibiting illiberal tendencies under the rule of authoritarian actors. The book demonstrates that SDIOs are not marginal to politics – they have become integral to governance strategies, particularly in contexts marked by democratic backsliding or geopolitical rivalry.

The global scope of this volume enables a comparative understanding of the practices, infrastructures, and tactics employed across varied regimes, with varied stages of digital authoritarianism. Chapters analyzing Thailand's military propaganda machine and Egypt's media ecosystem under Sisi reveal how governments increasingly rely on technologically mediated manipulation to assert control and deflect criticism. SDIOs function as part of broad toolkits of authoritarianism to manage opposition, orchestrate legitimacy, and influence international perception.

Simultaneously, the book brings attention to the activities of non-state actors who, while often operating with fewer resources, are no less impactful. Hacktivist groups, ransomware networks, digital mercenaries, and

ideological movements such as Al-Shabaab use SDIOs to disrupt, mobilise, and extract concessions. Their actions reflect the asymmetric potential of digital technologies, where tactical flexibility and creative messaging can substitute for and in some cases prove more impactful than formal institutional power. The comparative analysis of these actors illustrates the breadth of SDIO usage – from economic extortion to ideological warfare – making clear that the digital field is contested by multiple actors, not only sovereign states.

A particularly original theoretical contribution of the book is its examination of the intersectional and sociological implications of digital manipulation. Moving beyond the mechanics of misinformation and platform manipulation, the book foregrounds how SDIOs reshape collective identities, reinforce polarisation, and fracture shared realities. The chapter on Iran's "Women, Life, Freedom" protests, for example, explores how digitally orchestrated disinformation campaigns were used to delegitimise female-led resistance and enforce narratives of state victimhood. In Serbia, Russian-aligned disinformation, funneled through local media and political actors, reveals how information manipulation is sustained through elite networks and media ownership, not only through digital platforms alone.

These examples underscore the capacity of SDIOs to reconfigure the relationship between state and society. By weaponising emotional registers such as fear, resentment, and nostalgia, SDIOs provoke affective responses that can override deliberation, producing new loyalties and silencing dissent. This book offers a critical insight into this shift from rational persuasion to affective manipulation, shedding light on how SDIOs are calibrated to work not simply through information but through emotion, cultural memory, and symbolic political discourse.

The book also contributes to debates on audience agency and response. It emphasises that audiences are not passive recipients of content but interpret digital narratives through lenses framed by prior beliefs, identities, and digital literacies. Understanding how and why certain narratives take hold, and why others fail, is key to developing more effective countermeasures. Rather than prescribing simplistic solutions, the book advocates for critical thinking, civic education, and transparency in algorithmic design as essential elements of societal resilience.

An important methodological innovation of the book is its interdisciplinary approach. Contributors employ diverse research methods – including discourse analysis, field interviews, platform ethnography, and computational analysis – to trace the construction, circulation, and reception of SDIOs. This multifaceted approach allows the book to address not only the textual content of digital operations but also the infrastructures and networks that support their dissemination. Case studies from diverse sociopolitical settings, including Turkey, India, Hungary, Serbia, and Iran, among others, provide a

valuable comparative lens, offering insights that are applicable across regions while remaining sensitive to local contexts.

The volume also develops a conceptual framework for understanding the shifting dynamics between state and non-state actors in the digital ecosphere of governance and influence. While states often bring institutional power, legal authority, and long-term strategic planning, non-state actors tend to operate with speed, agility, and ideological commitment. The book traces how these actors converge, diverge, and at times even cooperate – creating a complex and fluid ecosystem of digital influence. It shows that the distinction between state and non-state is increasingly blurred, particularly when governments outsource SDIOs to proxy actors or when private firms engage in influence-for-hire practices.

Finally, the book addresses the broader implications of SDIOs for democratic governance and global security. As governments around the world adopt digital repression strategies, and as both illiberal and democratic regimes engage in narrative warfare, the space for open dialogue and factual debate continues to shrink. The book provides a timely warning of the long-term consequences of this trend, including the erosion of public trust, the normalisation of disinformation, and the weakening of international norms around freedom of expression and media pluralism.

Overview of the Book Chapters

The book is structured into five main parts: elections, conspiracy theories, digital authoritarianism, transnational dynamics, and non-state actors and extremism. Each part provides insight into different aspects of digital IO and their impacts on politics and society. This introduction (Chapter 1) is followed by 13 main chapters (Chapters 2–14) and a conclusion (Chapter 15). After the book unfolds the main themes and goals highlighted here in 13 main chapters, the conclusion then synthesises the ideas from the main chapters, offering suggestions for future research directions and policy blueprints. In this way, the volume becomes an exhaustive exploration of multifaceted realms of digital autonomy and coercion from a perspective that portrays the complicated linkages tied to technology, supremacy, and political trends among separate regions and contexts.

Part 1: Elections

In Part 1, on elections, we examine the role of SDIOs in shaping electoral outcomes and political communication strategies in Pakistan and Nigeria across two chapters, Chapters 2 and 3.

Chapter 2, titled "A Comparative Analysis of Pakistan's Digital Parties: Beyond Traditional Politics," by Ramsha Jahangir, investigates the influence

of social media on Pakistan's electoral terrain. This chapter analyzes the digital strategies employed by the country's two major political parties, the Pakistan Tahreek-e-Insaaf (PTI) and Pakistan Muslim League-Nawaz (PML-N) during the 2024 general election. While substantial evidence indicates the influence of online politics on voting outcomes, there is still a limited understanding of the interaction between formal and informal actors contributing to online political influence. The study posits that these often indistinct formal and informal party channels require scholarly attention, especially with 2024 being a year of elections. In this regard, the author draws from 195,736 posts by the political leaders, official accounts, digital media leads, and supporters of the two (aforesaid) political parties on X (formerly known as Twitter). This data collection process was carefully designed, which, on one hand, sought insights from ten (five each) "official" X accounts of the two parties (including the pages of party leaders), and, on the other hand, monitored the activity of 1,000 (500 each) party supporters and friends. This study disrupts the previous understandings of social media activity in Pakistan, which had highlighted the pivotal, almost solitary, role of "official" party and political leaders' accounts in mobilising supporters and setting relevant agendas. Although conventional political players continue to dominate the field of politics, this study presents concrete evidence that they are increasingly sharing the stage with emerging online actors who are critical to party discourse, even if they are not formal party members. These "non-electoral" actors affect politics through both direct and indirect means by coordinating their content with political figures in order to boost party messaging. The study discovered that, in addition to formal party outlets and leaders, social media followers play an important role in spreading party messaging. They run coordinated efforts and saturate online debate with a broader range of issues that are consistent with the party message. Based on the findings, the author calls for an increased focus on the role of these "new" digital actors, which are currently neglected in extant literature.

Chapter 3, "Dis/misinformation, Visibility Politics, Populism, and Digital Information: An Analysis of Pre- and Post-2023 Nigerian General Elections," by Najimdeen Ayoola Bakare, explores the impact of digital media on Nigeria's 2023 general elections. Using "politics of visibility" as a conceptual framework, the study touches on five areas in the larger context of misleading digital information and electoral politics in Nigeria. First, the author examines how disinformation and misinformation are strategically employed in tandem with identity politics and the politics of visibility. Second, the study analyzes the strategic manipulation of digital media to influence electoral outcomes, uniquely examining digital media's role in pre-election rigging as well. Third, Ayoola also touches on the role of digital media in advancing populist messaging, conspiracy theories, and misleading information that negatively targets opposition parties in election cycles. Additionally, the

connection between the content on digital media and the subsequent exacerbation of ethnic and religious divides, political polarisation, and separatism is also investigated. Lastly, the implications of the proliferation of digital media are also studied, especially in the context of Nigerian electoral politics. The findings suggest that in the 2023 Nigerian general elections, digital platforms were utilised as tools for driving change and fostering a shared identity among those dissatisfied with the past, critical of the present, and hopeful for a better future for Nigeria. This construction of a collective identity was strategically aimed at encouraging participation in political protests against the establishment. Additionally, during the election period, media content was not only toxic but also exemplified both misinformation and disinformation. The primary instigators of this misleading information over digital platforms were populist politicians who carefully tapped into existing fault lines, thereby sowing seeds of hatred and division.

Part 2: Conspiracy Theories

In Part 2, on conspiracy theories, we dive into modern conspiracy theories disseminated across various online platforms, through two main chapters (Chapters 4 and 5).

Chapter 4, "The Persistence of Informational Manipulation and the Appropriation of Emerging Events: Conspiratorial Publics," by Katherine M. FitzGerald, Timothy Graham, and Daniel Whelan-Shamy, provides an analysis of contemporary conspiratorial theories and their circulation on digital platforms, examining the roles of state and non-state actors in their dissemination in digital space. The larger purpose of the chapter is twofold. First, the authors delineate an exploratory analysis of 13,500 X posts, which were collected via exploratory digital methods during the 2023 Maui wildfires. Second, the authors grapple with the origination, nature, and circulation of conspiracy theories on digital platforms. The findings of the chapter suggest that the transient character of conspiracy theories and their potential to resurrect more established notions that comprise the "conspiratorial canon" are utilised on digital platforms as instruments of political manipulation and control. The counter-myths put forward by state actors and other political actors demonstrate this tendency, as they frequently revive conspiratorial narratives that support their positions in response to criticism. This, according to the authors, was clearly witnessed during the Maui bushfires, where opponents of the US government used old anti-Democrat conspiracies in addition to criticising the administration's present policies. By investigating the reasons for the persistence of some and the disappearance of other conspiratorial narratives in public discourse, this research fills a long-standing gap in the literature on digital IO and conspiracy theories. It is important to mention that this chapter proposes *conspiratorial publics*, a theory and a conceptual framework that attempts to shift the debate away from single cases to a

broader understanding of how conspiracy theories are formed on digital platforms. While the primary purpose of the framework is to understand the origination and sustenance of conspiracy theories, it can also help identify patterns and trends across conspiratorial communities. In this regard, this chapter makes a novel contribution that can burgeon the field of SDIOs in the context of conspiracy theories.

Chapter 5, "The Role of Social Media in the Diffusion of Conspiracy Theories and the Consolidation of Digital Authoritarianism in the Middle East: The Case of Egypt," by Ihsan Yilmaz, Ali Mamouri, and Shahram Akbarzadeh, explores the relationship between social media, conspiracy theories, and authoritarian politics in Egypt, highlighting the dissemination of anti-Western narratives and their impact on political stability. Using information from Facebook and YouTube as well as ten semi-structured interviews with key individuals, the chapter discusses three main conspiracy theories that acquired traction in Egypt following the 2013 coup. By adopting this technique, the contributors explore conspiracy theories that have surfaced in Egypt from Arabic-language materials after the Russian invasion of Ukraine, moving past the literature's predominant focus on Western states and English-language communication. The findings of the chapter suggest that three interrelated conspiracy theories have transpired in Egypt. First, Egypt's withdrawal from the International Grains Agreement in 2023 is understood as a Western attempt to starve and stifle Egypt. Second, the economic crisis in Egypt that has resulted from the Ukraine War is widely received by the public as a Western conspiracy to destabilise the country. Finally, the third conspiracy theory aligns with the 2023 presidential elections in Egypt, whereby it is believed that the Western powers are backing civilian candidates in opposition to President Abdel Fattah Al-Sisi. The alleged goal, in this regard, is to install a puppet president that serves the objectives of the Western powers. The book chapter posits that all three conspiracy theories position Egypt as an autonomous and powerful entity, Russia as an all-weather ally, and Western powers as the enemy. Furthermore, the results show that social media offers special advantages to the authoritarian state. The use of well-known internet personalities has not only helped the regime spread its claims to younger, more technologically literate populations but also helped in creating valuable conspiracy theories that implicate recognised allies like the International Monetary Fund (IMF) and the US without identifying them directly. Collectively, these conspiracy theories, according to the authors, are not just a standalone phenomenon but are rooted in the larger historical and geopolitical contexts.

Part 3: Digital Authoritarianism

In Part 3, on digital authoritarianism, we explore the use of digital space to empower authoritarian regimes across various regions, focusing on Thailand, Turkey, and Hungary, in three main chapters (Chapters 6–9).

Chapter 6, "#Propaganda: A Political Economy of SDIOs in Thailand," by Itsakul Unahakate, examines Thailand's state-led SDIOs, especially investigating the Thai military's efforts to manipulate public opinion and suppress pro-democracy movements. The chapter employs the Political Economy of the Media conceptual framework, specifically the "Propaganda Model," to analyze the Thai military's digital operations through five distinct avenues: ownership, advertising, sourcing, flak, and ideology. The chapter contends that understanding the dynamic nature of SDIOs itself is crucial to assessing the effectiveness of the army's digital operations. The players involved and their relationships with the changing environment – especially regarding communication technologies – should be fully comprehended. The author details that the information activities in Thailand have traditionally been carried out in large part by state entities, particularly by the military. These efforts, which have their roots in the anti-communist movements of the 1960s, are today experiencing challenges in influencing public sentiment because of the widespread use of social media and other communication technologies. It is witnessed that the Thai army is acquiring knowledge, adjusting, and normalising these digital-related activities, as seen by their recent deployment of SDIOs. The army has modified its policies in light of its new recognition of the significance of social media. Together with non-state actors, they have enhanced the use of SDIOs to successfully shape public opinion and sentiments. Additionally, the Thai military is working in tandem with the Pheu Thai Party, which now controls the nation, to normalise and control communication operations. The chapter demonstrates that in the setting of the Political Economy of the Media, reconsidering the Propaganda Model serves to highlight the task of generating consent. This construction of consent and approval is currently less successful on social networking platforms and the internet in comparison to similar efforts on conventional mass media. Nevertheless, Thai pro-democracy and civil rights groups remain vulnerable because state actors and their affiliates have access to both legal and intellectual weapons. These instruments might restrict the right to free speech and impede the country's democratic transition.

Chapter 7, "Turkish Government's Domestic Digital Information Operations on X (Twitter), Democracy, and Social Cohesion," by Ihsan Yilmaz, Bulent Kenes, and Nicholas Morieson, studies Turkey's domestic digital IO, analyzing their impact on democracy, social cohesion, and political stability. The chapter employs the case study of the Justice and Development Party (AKP), led by Turkish President Recep Tayyip Erdogan, to highlight the use of SDIOs by authoritarian governments. The chapter examines AKP's utilisation of digital tools like bots, hackers, and AK trolls to demonstrate how the internet world has become an essential platform for shaping political results and forming public opinion. Ideas like the establishment of

a "New Turkey," the development of Erdogan's personality cult, and the depiction of dissidents as domestic "others" serve as a direct by-product of the digital tools and illustrate the intricate nature of internet manipulation. Additionally, the authors contend that AKP-backed SDIOs, and the control of information that comes with it, have allowed the government to criminalise dissent and opposition as well. This is witnessed in the way dissidents and opposition voices are routinely targeted in Turkey, especially as seen in the brutal treatment of the Gezi protestors. Moreover, according to the authors, AKP's SDIOs have an emotive side as well, which is understudied in extant literature. These digital operations, especially when run by authoritarian governments, are designed to instill various kinds of emotions in the public, including, but not limited to, fear, anger, and resentment. On the back of these emotions, authoritarian governments like that of the AKP can rally support, target opposition groups, and discredit traditional media outlets. The chapter contends that this relationship between SDIOs and emotive mobilisation is pivotal and should be explored as part of future studies as well. Collectively, the chapter is an intriguing study of the extensive implications of SDIO, which are way more far-reaching than what meets the eye.

Chapter 8, "India's Strategic Digital Information Operations," by Ihsan Yilmaz and Chloe Smith, outlines the rapid transformation of India's digital sphere under the leadership of Prime Minister Narendra Modi and the BJP government. Once seen as a proponent of democratic, plural digital development, the Indian state has increasingly adopted authoritarian strategies to dominate online spaces. The ruling party has implemented a range of SDIOs designed to suppress dissent, manipulate public opinion, censor critical and oppositional voices, and reinforce its political power. The study uses four significant digital mobilisation events – the farmer's protests, Delhi riots, COVID-19 infodemic, and the 2019 and 2024 general elections – to contextualise and demonstrate how India's SDIO operations involve coercive legal measures, censorship, surveillance, internet shutdowns, and the mobilisation of troll armies and disinformation networks. These actions are aimed not only at silencing critics but also at manufacturing consent and shaping public perception through emotionally resonant and identity-driven narratives. The result is an information ecosystem skewed heavily in favor of the government, where opposition voices are marginalised or criminalised. Additionally, the chapter situates India's digital authoritarianism within a global context of declining democratic freedoms. It highlights how India's governance on digital platforms mirrors trends observed in hybrid or authoritarian regimes, yet operates uniquely within the façade of democratic institutions. This discussion sets the stage for a detailed exploration of the legal, technological, and ideological components of SDIOs, and their impact on media freedom, civil liberties, and social cohesion in India.

Chapter 9, "Media as Tool for Strengthening Authoritarian and Populist Tendencies in Central European Countries: A Case Study of Hungary," by Martin Solik and Jan Graf, explores how digital spaces are used to influence the public in regions such as Central Europe, specifically focusing on Hungary as a case study. The larger objective of this chapter is to examine how Hungary's public and private media are changing, with a particular emphasis on the main forces behind this development. It aims to show, via media analysis, how state-run media serve as tools to strengthen authoritarian inclinations and undermine democratic ideals. The chapter argues that the media evolution in Hungary is supported by three main mechanisms. The passing of legislation is the first step. Notably, the "Media and Press Freedom Act" of 2010 required the media to report in an equitable, impartial, and all-encompassing manner. However, because of its evident conflict with democratic ideals, this bill received harsh criticism from institutions such as the European Union. One of the main points of controversy was the creation of the Media Authority, whose officials were closely associated with the Fidesz party and were granted broad authority to enforce the legislation and levy heavy fines for violations. The authors argue that Fidesz changed the media environment to support their rule by using legislative measures to modify the constitution as a primary tool. The second important mechanism is coercion and pressure based on finance and funding. This tactic demonstrates how public money is distributed to benefit media organisations that align with the governing party, while non-governmental media are financially challenged and frequently subject to punishment. As a result, independent media outlets have become weaker and are eventually purchased by fresh owners who support Viktor Orbán's political goals. For instance, owners sympathetic to Orbán's policies have seized control of the TV2 television station and the *Népszabadság* newspaper. Such financial manipulation distorts the media terrain and limits the range of viewpoints and information that the general public may access. As a result, pro-government media now dominate the terrain, and opposing viewpoints are disregarded, endangering Hungary's democratic values. Political pressure is the third important mechanism. The sophisticated types of pressure tactics that are discussed in the chapter include the systematic harassment and humiliation of left-wing reporters and activists who disagree with Viktor Orbán's political position and philosophy. The autonomy and liberty of journalists are seriously threatened by the verbal abuse that these individuals often endure. Political persecution of journalists has continued for more than a decade and has become even more intense, making the climate unfriendly for independent media. Holistically, the findings of the chapter go a long way in demonstrating the role of authoritarian governments in enacting coordinated strategies to censor and vilify opposing voices on media platforms.

Part 4: Transnational Dynamics

In Part 4, on transnational dynamics, the contributors examine how authoritarian rulers in Iran, Russia, Turkey, and India leverage SDIOs to extend their influence transnationally and suppress dissent within diaspora communities, in three chapters (Chapters 10–12).

Chapter 10, "Iranian State-Sponsored Disinformation Against the Dissidents at Home and in Diaspora," by Shahram Akbarzadeh, Amin Naeni, Galib Bashirov, and Ihsan Yilmaz, investigates Iran's use of online disinformation campaigns to discredit influential dissidents and suppress opposition movements both at home and among the Iranian diasporas. The chapter examines the conduct of the Iranian regime in the backdrop of the 2022 "Women, Life, Freedom" protests. The authors argue that during a legitimate political crisis, the Iranian government constructed a "Big Lie" to strategically target their opponents. Two primary groups were identified and then targeted with the use of online disinformation by the Iranian state. These groups were critic celebrities inside the country and famous dissenters abroad. The larger goal of the Iranian regime was to discredit the opponents and showcase the Islamic State as the only viable option. The chapter shows that the Iranian religious leadership has attempted to control the populace by historically blaming all anti-regime actions and domestic difficulties on the US. However, this perspective is losing traction as the general population begins to question the authenticity of the anti-US discourse. Blaming the US for Iran's challenges has become redundant. In its stead, a new Big Lie has emerged, mostly in the digital domain, to strengthen the regime's message amid times of crisis. This Big Lie, embedded in the state-crafted SDIO, has been propagated by state-affiliated websites and pro-regime accounts on social media. The latter has often amplified the narratives produced by the former, attempting to persuade the Iranian people that there is no viable alternative to Islamic rule. To this end, these actors have targeted dissenting individuals with humiliation and character assassination, portraying them as dishonest and illegitimate. The implied point is that Iran's future is attached to the Islamic regime, devoid of which Iran would collapse.

Chapter 11, "The Influence of the Kremlin in the Media Space of Western Balkan Countries: A Case Study of Serbia," by Jan Graf and Martin Solik, studies how pro-Russian narratives, disinformation, and propaganda are spread in Serbia. The study shows that Russian misinformation content is heavily influenced by the current crisis in Ukraine. Even if Russian media is present in Serbia, the country's media ownership arrangement and general news environment – which are marked by monopolisation, political reliance, and a lack of transparency – greatly increase Russia's impact on the country. The widespread adoption of Russian accounts on the conflict in Ukraine by Serbian media sources not only further inflames the country's anti-Western

sentiment but also exacerbates the dissemination of Russian misinformation. As such, the already sympathetic media in Serbia makes Russia's efforts to sway opinion in Serbia much more durable and effective, with a lot less time and resources. The authors argue that in addition to the possibility of its European Union membership being threatened, Serbia runs the risk of Kremlin narratives continuing to be spread throughout the region unless its media laws are brought into compliance with EU standards. Misinformation from Russia is spreading widely, which has the potential to destabilise the Western Balkans and impede reform initiatives that are essential for EU membership. In this regard, the authors highlight various polls and surveys, which display the level of Russian support in Serbia. A significant portion of the Serbian population supports Russia's war in Ukraine and generally wants good ties with Russia even at the expense of EU membership. This trend, according to the authors, is worrisome and might amplify the supposed authoritarian surge in the country. Lastly, the authors call for further research on the influence of Russian narratives and IO in other Western Balkan countries.

Chapter 12, "The Transnationalisation of Strategic Digital Information Operations: Turkey and India," by Ihsan Yilmaz, Priya Chacko, Susan de Groot Heupner, and Anand Sreekumar, employs the SDIO concept to compare Turkey's and India's use of digital technologies for authoritarian governance, highlighting the tactics, tools, and methods used by both governments. As such, the wide international reach and implications of Turkish and Indian Strategic SDIOs are demonstrated in this chapter. Targets for these activities include transnational entities, other countries, and diaspora communities. Through their diasporas, which are important sources of money, votes, and international legitimacy, these SDIOs actively influence geopolitical discourses and coalitions. These activities, which are carefully planned and carried out, are vital tools used by government figures to both strengthen their national support base and methodically weaken and invalidate minority and opposing forces at home and abroad. The authors argue that a web of undemocratic rules and regulations that offer credibility to the deceptive strategies employed in digital warfare at the national and international levels contributes to the efficacy of SDIOs. The impact of such activities is further amplified by the cooperation of other parties, such as pro-government diaspora groups, internet trolls, cooperative political leaders, sympathetic journalists, international governmental organisations, and corporate sector companies. Beyond just focusing on diasporas, the chapter argues that these SDIOs also seek to stifle foreign media and politicians who disagree with or criticise the Turkish or Indian governments. The objective is to dominate the discourse and muzzle dissent. A culture of perpetual monitoring is fostered by the pervasive use of technical tracking and surveillance technologies on social media, which instills a dread of being wrongly accused of militancy for just voicing disagreement. This careless labeling creates a climate of distrust

and suspicion as well as social anxiety. Interestingly, this narrative of portraying opposition groups as "militants" has resonated well with the support base of the governments of both India and Turkey. This not only further jeopardises the security of the dissidents but also emboldens the governments in the two countries to clamp down on dissent and opposition.

Part 5: Non-State Actors and Extremism

In Part 5, on non-state actors and extremism, we examine how non-state actors use digital space, with a theoretical focus on the distinction between state and non-state actors in Chapter 13. Additionally, we investigate alt-right ideology and masculinity as case studies in Chapter 14.

Chapter 13, "Differences in the Utilisation of Digital Tools for Information Operations Between State and Non-State Actors," by Mohamed Ibrahim, presents a comparative analysis of the utilisation of digital tools for IO by both state and non-state actors, examining their respective strategies, motivations, and operational capacities. This chapter elucidates the divergent approaches, assets, and objectives that characterise these actors, highlighting the structural and strategic contrasts between them. While state actors demonstrate a high degree of intelligence, coordination, and strategic foresight, non-state entities tend to operate with greater flexibility and impulsivity. Understanding these distinctions is imperative for the development of effective countermeasures against malign digital activities. The chapter contends that state actors engage in coordinated and strategically driven IO, often targeting critical infrastructure and deploying sophisticated misinformation campaigns. State-led propaganda efforts are primarily aimed at the dissemination of false narratives, frequently intertwined with political objectives and the exploitation of social media ecosystems. Through an extensive review of scholarly analyses, Ibrahim delineates patterns of state-sponsored IO across various historical and geopolitical contexts. The study identifies prominent state actors, including China, Russia, Iran, and North Korea, known for their extensive cyber espionage, disruptive cyberattacks, and systematic targeting of vital infrastructure. Conversely, the chapter illustrates that while non-state actors may possess advanced technological expertise, their resource limitations often necessitate alternative modes of operation, such as serving as proxies for state actors. The unpredictability of non-state actors stems from their diverse objectives, which frequently include financially motivated cyber offenses such as extortion attacks. The increasing adoption of offensive cyber capabilities by non-state entities complicates mitigation strategies, as these actors leverage asymmetric tactics to achieve their goals. Moreover, state-sponsored proxy warfare enables governments to outsource cyber operations to non-state groups, thereby lowering the threshold for engagement in contemporary digital

conflicts while maintaining plausible deniability. Ultimately, this chapter provides a critical examination of the dynamic terrain of IO, offering a complex understanding of the relationship between state and non-state actors in cyberspace. It contributes to the broader discourse on cybersecurity, digital warfare, and the implications of these operations for global security and geopolitical stability.

Chapter 14, "Digital Dissonance: Alt-Right Ideology, Masculinity, and the Strategy of Information Operations," by Aiden Aylett, Toija Cinque, and Jodi McAlister, dives into the digital strategies employed by alt-right podcasts to promote far-right ideologies, with a focus on the role of masculinity and opposition to mainstream political correctness. The chapter uses word frequency analysis alongside the BITE model, which as an authoritarian control conceptual framework breaks down the analysis into four parts: behavior, information, thought, and emotion. "The Ben Shapiro Show," "Tate Speech," and "The Alex Jones Show" are among the podcasts that the authors examine and find to have varied degrees of affiliation with alt-right ideology. Although, according to the authors, these podcasts cannot be overtly called alt-right, they act as a bridge to further radicalisation by adjusting and desensitising their primarily young male viewers to alt-right beliefs. According to the findings, these podcasts employ a variety of BITE model strategies to unduly impact their listeners, especially regarding alt-right ideas and philosophies. The chapter notes that on the authoritarian/destructive end of the impact, spectrum sat "The Alex Jones Show" and "Tate Speech," whereas the episodes of "The Ben Shapiro Show" conveyed comparable ideological notions in a less assertive way. Each of these three podcasts uses the charm of their hosts to spread false facts and information, which makes listeners distrustful of journalists and media organisations that disagree with their points of view. An "acceptable" or an appropriate type of masculinity is presented compared to the "unacceptable" version in each of the episodes examined in the chapter. The authors find that these podcasts exploit parasocial closeness as a hypnotic tactic to build strong bonds between hosts and the audience. The hypnotic impact of this strategy, together with the presenters' vocabulary and delivery manner, causes their audience to become accustomed to listening to these podcasts on a regular basis. To authors conclude that these podcasts possibly enable young men – a group that each program explicitly targets – to become more radicalised.

Chapter 15, "Future Directions in Strategic Digital Information Operations and Warfare," by Ihsan Yilmaz, details the main conclusions drawn from the several chapters of the book. The chapter synthesises the insights from the preceding 14 chapters, offering suggestions for further research and policy recommendations to address the challenges posed by digital IO in contemporary political terrains. The author offers several ways of dealing with SDIOs. They write to effectively counteract the negative impacts

of SDIOs; it is important to comprehend the perceptions and reactions of audiences. Encouraging analytical thinking, technological proficiency, and digital media literacy equips people to negotiate the potentially deceptive world of misleading information. Furthermore, the capacity to distinguish between truth and deception will be enhanced by implementing specialised fact-checking activities in conjunction with existing digital technologies that are transparent and accountable. Governments, tech corporations, and civil society organisations working together can create strong barriers to manipulation that protect democratic debate and allow for informed public involvement. Lastly, the chapter highlights the importance of burgeoning the field of SDIOs. This expansion not only would assist the general public in deciphering misinformation but can also allow global governments to enact effective countermeasures. As such, the authors call for further future research on SDIOs, especially with the use of complex and human-centered methodologies and multiple case studies.

Funding: *This work was supported by Australian Research Council [Grant Number DP230100257] and Gerda Henkel Foundation [Grant Number AZ 01/TG/21].*

References

Ahmed, Z. S., Yilmaz, I., Akbarzadeh, S., et al. (2024) Contestations of internet governance and digital authoritarianism in Pakistan. *International Journal of Politics, Culture, and Society*. https://doi.org/10.1007/s10767-024-09493-2

Akbarzadeh, S., Mamouri, A., Bashirov, G., Yilmaz, I. (2025). Social media, conspiracy theories, and authoritarianism: Between bread and geopolitics in Egypt. *Journal of Information Technology & Politics*, 1–14. https://doi.org/10.1080/19331681.2025.2474000

Akbarzadeh, S., Naeni, A., Bashirov, G., Yilmaz, I. (2024b). The web of big lies: State-sponsored disinformation in Iran. *Contemporary Politics*. https://doi.org/10.1080/13569775.2024.2374593

Akbarzadeh, S., Naeni, A., Yilmaz, I., Bashirov, G. (2024a, March 14). Cyber surveillance and digital authoritarianism in Iran. *Global Policy*, 1–11.

Bakir, V., McStay, A. (2018). Fake news and the economy of emotions: Problems, causes, solutions. *Digital Journalism*, 6(2), 154–175.

Chen, X., Valdovinos Kaye, D. B., Zeng, J. (2021). # PositiveEnergy Douyin: Constructing "playful patriotism" in a Chinese short-video application. *Chinese Journal of Communication*, 14(1), 97–117.

Dawoud, K. (2023). *Power cuts in Egypt: A political liability for Sisi ahead of the upcoming elections*. Middle East Institute. https://www.mei.edu/publications/power-cuts-egypt-political-liability-sisi-ahead-upcoming-elections

Hatch, B. (2019). The future of strategic information and cyber-enabled information operations. *Journal of Strategic Security*, 12(4), 69–89.

Ingram, H. J. (2015). The strategic logic of Islamic State information operations. *Australian Journal of International Affairs*, 69(6), 729–752.

Iwuoha, V. C. (2020). 'Fake news' and 'half-truths' in the framings of Boko Haram narrative: Implications on international counterterrorism responses. *The International Journal of Intelligence, Security, and Public Affairs*, 22(2), 82–103.

Mason, M. (2022). The price of propaganda: Inside Beijing's mission to drown out dissent. *AFR*. https://www.afr.com/technology/the-price-of-propaganda-inside-beijing-s-mission-to-drown-out-dissent-20220905-p5bfdv

Michaelson, R. (2018). 'No puppet': Last challenger in Egypt's election says he's more than a veneer of democracy. *The Guardian*. https://www.theguardian.com/world/2018/mar/20/egypts-ghad-party-leader-makes-discreet-bid-for-presidency

Mir, A., Mitts, T., and Staniland, P. (2022). Political coalitions and social media: Evidence from Pakistan. *Perspectives on Politics*, 1–20.

Perloff, R. M. (2021). *The dynamics of political communication: Media and politics in a digital age*. Routledge.

Postill, J. (2018). Populism and social media: A global perspective. *Media, Culture & Society*, 40(5), 754–765.

Sabbagh, D. (2020, September 29). Trump 2016 campaign 'targeted 3.5m black Americans to deter them from voting'. *The Guardian*. https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting

Starbird, K., Arif, A., Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–26.

Theohary, C. A. (2011). *Terrorist use of the internet: Information operations in cyberspace*. Diane Publishing.

Tokdoğan, N. (2020). Reading politics through emotions: Ontological ressentiment as the emotional basis of current politics in Turkey. *Nations and Nationalism*, 26(2), 388–406.

Walker, S. (2017). Russian troll factory paid US activists to help fund protests during election. *The Guardian*. https://www.theguardian.com/world/2017/oct/17/russian-troll-factory-activistsprotests-us-election

Yilmaz, I. (2021). *Creating the desired citizen: Ideology, state and Islam in Turkey*. Cambridge University Press.

Yilmaz, I., Akbarzadeh, S, Abbasov, N., Bashirov, G. (2024). The double-edged sword: Political engagement on social media and its impact on democracy support in authoritarian regimes. *Political Research Quarterly*. https://doi.org/10.1177/10659129241305035

Yilmaz, I., Akbarzadeh, S., Bashirov, G. (2023, September 10). Strategic digital information operations (SDIOs). *Populism & Politics (P&P)*. European Center for Populism Studies (ECPS). https://doi.org/10.55271/pp0024a

Yilmaz, I., Albayrak, I. (2021). Instrumentalization of religious conspiracy theories in politics of victimhood: Narrative of Turkey's directorate of religious affairs. *Religions*, 12(10), 841.

Yilmaz, I., Demir, M. (2023). Manufacturing the Ummah: Turkey's transnational populism and construction of the people globally. *Third World Quarterly*, 44(2), 320–336.

Yilmaz, I., Morieson, N., Shakil, K. (2025). Authoritarian diffusion and sharp power through TV dramas: Resonance of Turkey's 'Resurrection: Ertuğrul' in Pakistan. *Contemporary Politics*. https://doi.org/10.1080/13569775.2024.2447138

Yilmaz, I., Shakil, K. (2025). *Reception of soft and sharp powers: Turkey's civilisationist populist TV dramas in Pakistan*. Singapore: Palgrave Macmillan.

Yilmaz, I., Shipoli, E. (2022). Use of past collective traumas, fear and conspiracy theories for securitization of the opposition and authoritarianisation: The Turkish case. *Democratization*, 29(2), 320–336.

PART 1
Elections

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

2

A COMPARATIVE ANALYSIS OF PAKISTAN'S DIGITAL PARTIES

Beyond Traditional Politics

Ramsha Jahangir

Introduction

The year 2024 witnessed an abundance of elections in 40 countries, with 41% of the world's population preparing to vote in some capacity (Curran and Crawford 2023). During this high-stakes election year, governments and political parties leveraged technology to employ an array of SDIO tactics to influence public discourse and counter opposing narratives online. While the use of technology was previously limited to new or less established parties, the rise of tech-savvy voters has pushed traditional actors to tap into the new affordances of digital platforms. The 2024 voter has migrated from "neighbourhood parks to WhatsApp groups, which now serve as their digital gathering spaces" (Dutt 2024). Researchers have also linked the significant use of digital platforms such as Twitter to the winning party's electoral success (Ahmed, Jaidka, and Cho 2016; Batool et al. 2022; Mulla 2017).

In digital campaigns, where "politics of visibility" and influence drive electoral success (see Chapter 3 by Najimdeen Ayoola Bakare), political parties are turning to new digital players such as paid or volunteer supporters to help them connect with the public. These online supporter networks have not only helped governments and political parties build support (Abrahams and Leber 2021; Tshuma, Tshuma, and Ndlovu 2022; Mir, Mitts, and Staniland 2023) but also been used to attack and fact-check journalists (Mulla 2017; Jahangir 2021), and drown out countering narratives (Hussain, Shahzad, and Saud 2021).

As supporter networks have become a central plank in political communication (Shih 2023), this chapter aims to study their role through the lens of the coalition approach proposed by Mir, Mitts, and Staniland (2023). As

DOI: 10.4324/9781003628088-3
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

established by Mir, Mitts, and Staniland (2023, 1340), online dynamics comprise a wide range of actors who contribute to party campaigns for various reasons, some based solely on support and some as part of a coordinated effort to manage the public sphere. For instance, a study by Abrahams and Leber (2021) found that a significant portion of pro-regime content online originated from grassroots efforts of pro-Saudi supporters rather than being driven by state officials.

Despite evidence of digital campaigns shaping elections, little is known about the relationship between formal and informal actors in IO. These, often blurred, formal and informal party channels require academic attention, particularly during a global year of elections. While research has extensively studied politicians' social media use during elections (Batool et al. 2022; Ahmed and Skoric 2014), this chapter broadens the focus to party social media managers and their followers, providing insights into new political party communication structures. Previous studies suggest that newer parties effectively use Twitter for voter engagement, unlike mainstream parties (Batool et al. 2022; Ahmed and Skoric 2014; Mulla 2017; Ahmed, Jaidka, and Cho 2016). This analysis examines the core Twitter accounts and networks of leaders from Pakistan's two largest parties (Pakistan Tehreek-i-Insaf and PML-N) during the contested 2024 elections. Using narrative alignment and coordination indicators, it further explores political actor interactions during a major power transition. Mir, Mitts, and Staniland (2023, 1338) in their research on the 2018 general election noted a "high degree of complexity and opacity in Pakistan's politics." Since 2018, Pakistan has experienced significant political upheaval. Former Prime Minister Imran Khan, founder of the Pakistan Tehreek-i-Insaf (PTI), was ousted and jailed after a dramatic fallout with the military. Subsequently, the opposition PML-N and Pakistan Peoples Party (PPP) formed a coalition government. Given the PTI's prior alliance with the military and its dominance online in 2018, it's important to analyze how online dynamics have shifted with this change in political alignment.

This chapter examines how political leaders engage with formal and informal channels and the coordination of their communication. Analyzing 195,736 tweets from January 10 to February 10, 2024, it applies a coalitional approach to compare PTI and PML-N's reliance on official leader accounts versus their social media networks in the 2024 elections.

New Forms of Social Actors

Despite the growing popularity of social media and politics research, the increasing role of party influence networks remains a relatively under-explored area, especially within complex multi-actor political environments like Pakistan.

Scholars have extensively studied the use of social media by politicians for authoritarian censorship (Gohdes 2020; Yilmaz et al. 2022), election campaigns (Chhibber and Ostermann 2014; Ahmed and Skoric 2014), to spread cyber hate (Siddiqua 2021), and lead disinformation and propaganda campaigns (Hussain, Shahzad, and Saud 2021; Schliebs, Howard, and Bailey 2021). There is also ample research exploring the role of social media in protest movements (Munger et al. 2019) and why Twitter is a popular choice for politics (Ahmed, Jaidka, and Cho 2016; Batool et al. 2022). Despite the growing body of work focusing on the use of social media by political actors for various purposes outlined earlier, very few researchers are directly navigating how major political actors and their associated networks engage in the online sphere (Mir, Mitts, and Staniland 2023).

Due to the multitude of strategies adopted by political actors in the digital environment, there is a constellation of terms researchers use to describe influence networks. Most of the existing work looks at political support from paid actors referred to as "trolls" (Hussain, Shahzad, and Saud 2021; Yilmaz et al. 2022), "cyber troops" (Bradshaw and Howard 2018, 11), or "web brigades" (Tshuma, Tshuma, and Ndlovu 2022, 2–3). Another popular disinformation creator is automated accounts referred to as "bots" or "electronic armies" (Abrahams and Leber 2021, 1174). Researchers have spent a lot of time trying to distinguish between humans or bots participating in social media campaigns and amplifying political content on Twitter (Howard and Kollanyi 2016; Freelon and Wells 2020). Literature suggests that cyber troops are state-sponsored actors tasked with conducting disinformation campaigns online (Bradshaw and Howard 2018, 24). They may employ an inventory of manipulation strategies, including the use of automation such as political bots, and data analytics to amplify content posted under coordinated hashtag campaigns to spread hate speech or deceive the public (Bradshaw and Howard 2018; Bradshaw, Bailey, and Howard 2021). Some researchers argue that cyber troops may also deploy "trolls" to create multiple accounts that help attack or report content from opponents and critics of a party or government (Bradshaw, Bailey, and Howard 2021; Freelon and Wells 2020). For instance, in Pakistan, coordinated groups have artificially boosted political campaigns and mass-reported hashtags to prevent them from trending.

Disinformation and information warfare researchers have found that governments rely on the purposeful use of cyber troops due to cheap human resource (especially in developing countries) and their effectiveness in countering enemy narratives, as well as distributing content globally (Hussain, Shahzad, and Saud 2021; Cheema 2020; Jorgic and Pa1 2019; Fahmy 2017; Schliebs, Howard, and Bailey 2021). Bradshaw, Bailey, and Howard (2021, 8) found evidence in 61 countries of political parties or politicians running for office using a propaganda strategy led by cyber troops.

Though paid troops remain a concern, recent research is shifting its focus. The emphasis is now on exploring the decentralised efforts of online supporters, suggesting a more complex understanding of online influence. In their research on pro-Saudi online supporters, Abrahams and Leber (2021, 1191) argue against the perception that pro-Saudi influence networks were dominated by bots. Instead, they invite research into a more complex rarified class of influencer accounts termed "cyber knights," who may appear to be fewer in numbers but enjoy a large following, and their considerable clout helps influence political discourse online (Abrahams and Leber 2021, 1192).

The findings are echoed in other research on new trends in social media politics. In Zimbabwe, researchers found that not all *Varakashi* (online supporters of the ruling party) were political trolls or cyber bullies (Tshuma, Tshuma, and Ndlovu 2022, 2–3). Social media, they argue, has created a "virtual community of dissent that actively fostered counter-hegemonic discourses" (Tshuma, Tshuma, and Ndlovu 2022, 4). Others have focused on the impact of "third-generation" social media strategies – such as populating the online space with competing narratives – employed during protests to divert public attention (Munger et al. 2019, 816). In India, researchers have studied the role of "diffuse actors" with no institutional or organisational affiliations as vote mobilisers during elections (Sinha 2023; Chhibber and Ostermann 2014; Ahmed, Jaidka, and Cho 2016).

While scholarly evidence is still limited, emerging research highlights the growing importance of *influencers* and other new social actors in the digital information sphere (Lobera and Portos 2021). As the intersection of traditional politics and digital communication evolves, Borucki and Fitzpatrick (2021, 6) view political parties as political networks. To better understand these networks, Gibson, Greffet, and Cantijoch (2017, 3–5) propose three different forms of party membership in the context of digital affiliation within political parties: *Digital activists* (those who formally and visibly identify as supporters), *Friends* (follow official channels on social media and also engage in discussions), and *Audience* (follow party channels but have not made their support public or visible). The categories are not mutually exclusive, and can also overlap (Gibson, Greffet, and Cantijoch 2017, 3–5). The approach reveals that "digital channels may be providing a new space for party politics to occur" and have engaged individuals "who may not have traditionally engaged with parties through traditional membership" (Gibson, Greffet, and Cantijoch 2017, 3–5).

Given the changing political terrain, there is a growing call for exploring the role of new social actors who may or may not be directly affiliated with a political party. To study how parties and leaders interact with a broad constellation of actors that are not directly part of formal parliamentary politics, Mir, Mitts, and Staniland (2023) propose a coalitional approach. In line with other literature, they contend that content in the multisided and

multidimensional digital environment may not always be directly manipulated or controlled by the state. The coalitional framework is therefore useful in analyzing politics at play when there is a "greater premium on crafting strategies of narrative support and 'swamping' that does not rely primarily on tools of direct control" (Mir, Mitts, and Staniland 2023, 1338).

Pakistan 2024 Elections and Digital Politics

This chapter empirically focuses on the February 8, 2024, Pakistan election, which was held after two years of political turmoil and a month's delay. In 2022, the military-Khan conflict broke out following his government's ouster by a no-confidence motion which he believed was a well-coordinated plan led by the military together with the US for a regime change. Khan's party came under scrutiny on May 9, 2023, after its supporters launched attacks on military bases across Pakistan. Since 2023, Khan has been in custody being charged with multiple corruption cases and mishandling classified information, which meant he could not campaign for his party in the election. Notably, in the lead-up to elections, the Supreme Court of Pakistan refused to award the PTI its long-time election symbol, a cricket bat, a move widely perceived to be an effort to tilt the playing field against the party. The ruling coincided with a severe government crackdown on the PTI over the past year, with thousands of party members jailed and nearly all of its senior leadership being coerced to exit politics. Additionally, the party faced media and internet censorship and limitations on campaigning in the lead-up to the election (Afzal 2024; Mir and Salikuddin 2024). On election day, internet and mobile services were shut down. Access to Twitter was also disrupted for over a month after election results were announced. The EU, US, and the UK noted a lack of a level playing field in the 2024 election, attributing that to the inability of some political actors to contest the elections and to restrictions on freedom of assembly, freedom of expression, and internet access (Singh 2024).

In response to the challenges encountered by the PTI in campaigning, the party adopted a "systematic and contemporary approach, leveraging artificial intelligence and social media proficiently" (Afzal 2024). PTI's innovative technology playbook to bypass censorship featured strategies such as organising *virtual jalsas* on Twitter, crowdsourcing data for canvassing, and leveraging social media platforms such as TikTok and YouTube to engage voters despite a media blackout (Jahangir 2023). In contrast, the PML-N was criticised for its old-fashioned approach to election campaigns and for failing to adapt to technology and convince tech-savvy voters (Afzal 2024). The PTI's digital prowess played a crucial role in its electoral success despite the state crackdown and censorship, confirming the role of technology in contemporary politics: Independents backed by the PTI won the most seats

at the national level. Despite Khan's popularity, the second and third-largest parties in parliament, the PML-N and PPP, formed a coalition government. The outcome of the polls points to a more complex political DNA controlled by the powerful military. This chapter, however, centers on the important role of party supporters online in contributing to one of the biggest political upsets in the country's history.

PTI's digital strategy has not only disrupted the traditional status quo but also set a new benchmark for electoral campaigns around the world (Jahangir 2023). Previous research has documented PTI's large online presence and shown the impact of its effective information sharing on Twitter during past elections (Batool et al. 2022; Mufti, Shafqat, and Siddiqui 2020; Mulla 2017; Ahmed and Skoric 2014). Drawing parallels to Barack Obama's 2008 campaign, scholars have noted how PTI's social media team drew younger Pakistanis to politics, who were otherwise frustrated with a political system rooted in dynastic and tribal loyalties (Mulla 2017; Ahmed and Skoric 2014; Yilmaz et al. 2022). In the 2018 election, Mufti, Shafqat, and Siddiqui (2020, 12) observed, "Learning from PTI's success, other parties sought to emulate these strategies [using social media] in advance of the 2018 election – strategies that were aided by the introduction of 3G and 4G mobile broadband internet in Pakistan." Not only was Imran Khan the first Pakistani premier to use social media for official communication, but the PTI government was also the first to formally establish a digital media wing within the Prime Minister's Office. During his tenure, PTI's Imran Khan continued to benefit from the support of thousands of online supporters based around the world to build a positive perception of his governance (Jahangir 2020). The tech-savvy social media network of PTI not only helped build its own brand but also helped the military in perception management by crafting campaigns to amplify narratives in line with foreign policy and national security (Jahangir 2022).

While widely acknowledged, the political efficacy of the PTI's social media supporter base was downplayed in popular discourse, and its ability to translate into electoral victory was questioned (Jahangir 2022). The 2024 election, however, turned the tide. Despite facing an uneven playing field, not only PTI-backed candidates secured a majority of votes but the party's social media team successfully managed to run a global campaign against state repression and authoritarianism. It is worth noting that Pakistan has been downgraded to an authoritarian regime by the Economist Intelligence Unit.

With the major shift in Pakistan's political terrain and the important role of digital politics, there is an opportunity to explore how the systematic change in political alignments reflects in the online sphere. In 2018, "the playing field was tilted against the PML-N by a military with a long-standing distrust of the party; it censored the media, instigated anti-government events, and nudged independent political candidates to join the PTI" (Mir, Mitts, and Staniland 2023, 4). The researchers found the PML-N's social media network retweeted accounts that were more critical of the army's involvement in

politics and also had some alignment with dissidents. They found evidence of a de facto coalition between the military and PTI (Mir, Mitts, and Staniland, 2023). Now, with the PTI's fallout with the military and the PML-N's return to power, this chapter aims to explore the shift in narrative alignment and to what extent it is prominent in the official communication of the two parties and unofficially via their online supporters. The focus is on PML-N and PTI given they've been both on the receiving end of state authoritarianism and benefitted from military support to win elections. The two parties also are Pakistan's biggest digital parties – comprising a large official and unofficial supporter base on social media, particularly on Twitter (Jahangir 2022). While previous studies have looked at leadership accounts of political parties during election periods, specifically content posted by PTI's leadership on Twitter, this chapter aims to broaden the scope by also analyzing the strategies employed by party social media managers alongside online supporter accounts for PTI and PML-N.

Based on the coalitional approach proposed by Mir, Mitts, and Staniland (2023), the following sections pursue three goals: (1) identify prominent topics that official party channels and their networks promoted during the election period, (2) assess the degree of similarity in terms of the content they post on Twitter, and (3) explore to what extent these actors coordinate content to understand the role official party actors and their supporters play in digital communication.

Methodology and Results

Data Collection and Curation

Data were collected from Twitter using Python. To explore the multi-actor ecosystem of each party, I identified two types of party channels: *core accounts* (five official party channels selected based on their leadership roles and centrality to the 2024 election) and *follower accounts* (500 accounts that posted the most replies to or retweets from each party's core accounts). Based on the typology by Gibson, Greffet, and Cantijoch (2017, 3–5), the 500 follower accounts were divided into two groups: digital activists (followers with explicit mentions of PTI or PML-N in their bios or usernames) and party friends (the remaining highly engaged followers who lacked direct affiliation).

To analyze the social media activity of prominent party channels, I selected five key Twitter accounts from each of the PTI and PML-N parties. Each party's set of accounts included party leaders, social media managers, and the party's official Twitter page. Selected PTI accounts were official Twitter channel (@PTIofficial), PTI leader Imran Khan (@ImranKhanPTI), PTI chairman (since Dec 2023) Gohar Ali Khan (@BarristerGohar), PTI senior vice president Sher Afzal Marwat (@sherafzalmarwat), and PTI's social media

TABLE 2.1 Designation, username, number of tweets, and mean engagement metrics for the ten core accounts.

	Designations	*Account*	*Tweets*	*Mean Retweets*	*Mean Replies*
PTI	Official Account	PTIofficial	4,085	1,651.6	85.1
	Leaders	ImranKhanPTI	34	27,425.3	2160.2
		BarristerGohar	15	4,027	258.8
		sherafzalmarwat	356	3,503.6	203.4
	Social Media Head	agentjay2009	213	1,445.8	92.1
PML-N	Official Account	pmln_org	2,005	172.3	57.3
	Leaders	CMShehbaz	41	1,471.5	676.0
		Marriyum_A	168	339.8	183.9
		MaryamNSharif	260	915.7	461.9
	Social Media Head	Atifrauf79	450	186.6	33.7

lead Jibran Ilyas (agentjay2009). Selected PML-N accounts were PML-N's official Twitter channel (@pmln_org), PML-N leader Maryam Nawaz Sharif (@MaryamNSharif), PML-N president Shehbaz Sharif (@CMShehbaz), PML-N's information secretary Marriyum Aurangzeb (@Marriyum_A), and PML-N's social media head Atif Rauf (@Atifrauf79).

To analyze the interactions with these core party channels, I identified 500 follower accounts which sent the most replies to or retweeted content from each party's core accounts in the lead-up to the election.

All tweets from core and follower accounts were scraped for the 31 days leading up to the election (January 10–February 9, 2024). This yielded 4,703 and 2,924 from PTI and PML-N core accounts, respectively (Table 2.1). PTI's five core accounts received significantly more engagement than PML-N's five core accounts. Specifically, 332,115 unique accounts interacted with PTI content, while only 71,591 interacted with PML-N content. PTI followers posted 107,751 tweets, and PML-N followers posted 118,892 tweets.

The tweets were filtered by two criteria: (1) language (only tweets in English were included) and (2) keywords (only tweets that contained keywords related to one of the main topics of the election were included).

In total, the resulting dataset consisted of 3,891 tweets made by PTI's core accounts, 2,657 tweets made by PML-N's core accounts, 86,513 tweets made by PTI digital activists and party friends, and 102,675 tweets made by PML-N digital activists and party friends.

Topics and Discourse

To identify dominant online topics during the 2024 elections, I adapted the keyword list from Mir, Mitts, and Staniland (2023) to reflect the current political climate. The resulting topics were PTI and PML-N (mentions

and discussion), economy, corruption, human rights (including censorship), the judiciary and courts, foreign policy (covering Palestine, the Taliban in Afghanistan, and relations with the US, China, and Saudi Arabia), military involvement in politics, militancy, relations with India, media (including social media access), and the 2024 elections themselves. See the Appendix for a full list of keywords used for each topic.

To see how different actors prioritised and engaged with these key topics, I calculated the proportion of tweets made by each actor type per topic (number of topic-related tweets divided by the actor type's total tweet count; Figure 2.1).

Figure 2.1 shows that foreign policy was the most prominent topic on Twitter, and that the proportion of tweets by PML-N on the topic was higher than that of PTI. Interestingly, for PML-N, the conversation was led by its official page as opposed to party leaders. There were also significant contributions on this topic by PML-N's friends and digital activist networks. PTI likewise engaged heavily on the topic of foreign policy but with a smaller proportion of posts than PML-N. Both parties also posted frequently on the topic of the media (including mentions of social media platforms), but PTI prioritised the topic more than PML-N. PTI's social media manager most frequently tweeted about the media followed by the PTI's leaders, friends, and digital activists. Overall, there was also prominent engagement by social

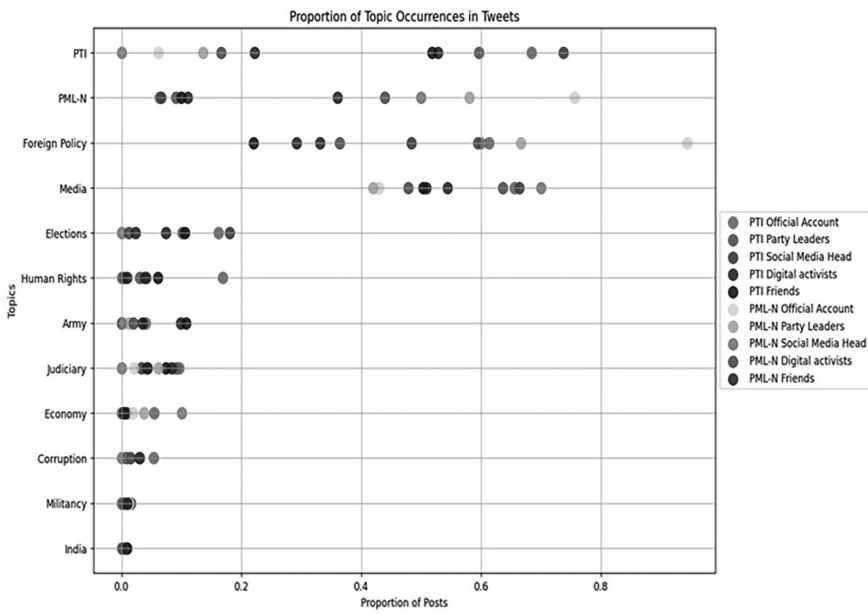


FIGURE 2.1 The proportion of posts about each topic is shown for each type of political actor within PTI and PML-N.

media managers, digital activists, and friends networks in conversations about their respective parties and leadership.

In terms of topics, issues related to militancy, the economy, corruption, and India were less salient during the 2024 elections. PML-N overall engaged on relatively fewer topics than PTI. PTI talked about a broader spectrum of political issues than PML-N, including human rights, judiciary, the elections, and the army.

In terms of topics advanced per actor, it was found that all PTI actors prioritised discourse about PTI, foreign policy, and the media. This indicates narrative alignment and coordination to some extent, as these actors generally engaged on the same topics, although to different degrees. It is worth noting that while PTI's official channels, including the social media head, also advanced posts about broader political issues such as elections and human rights, supporter networks added posts about PML-N, corruption, and the army's involvement in politics. Interestingly, it was PTI friend networks and digital activists who posted about the army. For PML-N, the top three topics were likewise foreign politics, the media, and the party itself. As with PTI, there were clear differences in which topics PML-N prioritised across the official channels and support networks. Unlike PTI, the PML-N's digital activists and party friends did not post more about the party itself than on the official channels. The only other topic that PML-N engaged consistently on was PTI, indicating that PML-N engaged on a smaller set of topics than PTI. While both PTI and PML-N prioritised posts about their own party instead of the opposition, posts related to the opposition were most frequently generated by digital activists, party friends, and social media heads.

Narrative Alignment

The topics political actors prioritise on social media reveal key themes in their communication but not details about their messaging style. Although different actors can discuss the same issues, their framing often differs. Therefore, I used a semantic similarity approach to assess narrative alignment within each party. Tweets were converted into word embeddings, and cosine similarity was calculated to measure textual overlap. Higher similarity values indicate more unified communication, while lower values suggest dissimilar or conflicting narratives.

Figure 2.2 illustrates how closely the narrative of political actors in each party aligned. Each plot represents the narrative alignment between tweets made by two actor types within the political parties. The figure presents two ways to assess this alignment: black dots and red lines. Each black dot represents the semantic similarity between a pair of tweets from two actors on a given day, while the red trend lines track the daily average similarity between the two actors.

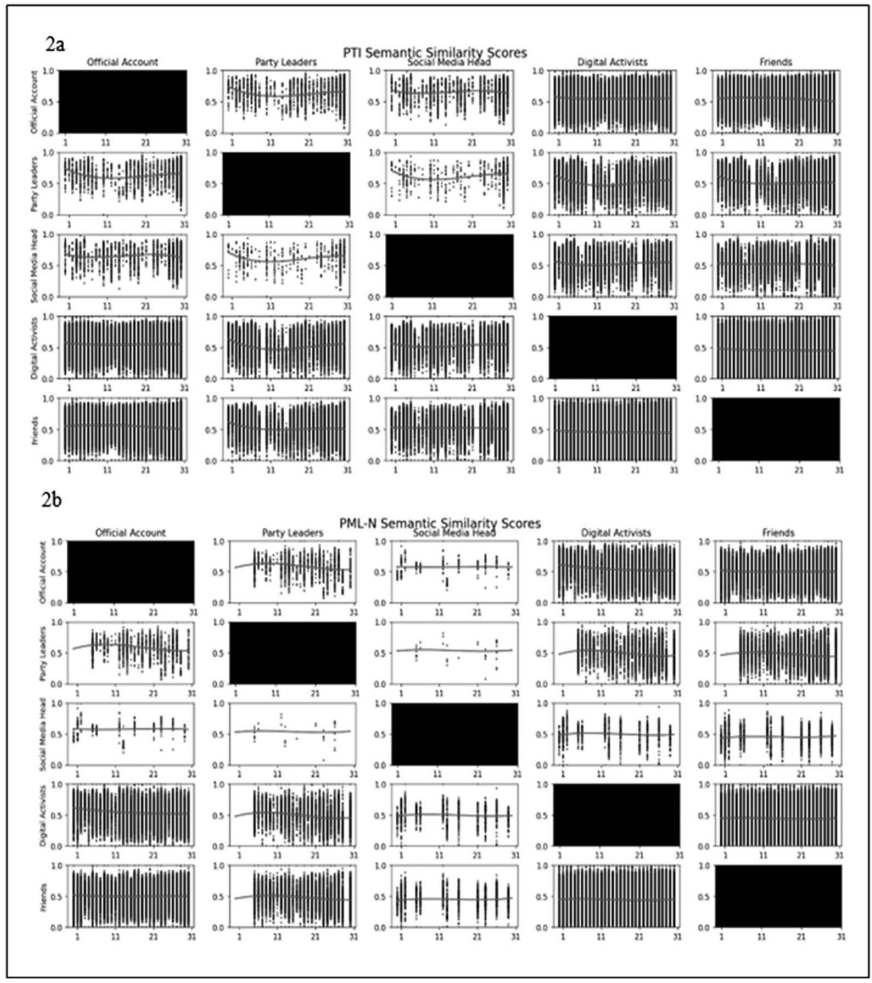


FIGURE 2.2 Semantic similarity per day in the month leading up to the election.

Note: Some dates do not contain any data. On these dates, one of the two actors in the actor pair had made no tweets. 2a shows the data for PTI. 2b shows the data for PML-N

Overall, the trend lines indicate that party messaging was generally similar throughout the election period, with most actor pairs having similarity scores slightly above 0.5 throughout the month. Similarity scores between core party accounts were generally higher, especially within PTI. In addition, PTI's social media head was well aligned with both official party channels and supporters, whereas PML-N's social media head was less active and showed less alignment with other PML-N actors. Core accounts in both PTI and PML-N showed stronger narrative alignment with digital activists at the start of the

month. However, the narrative similarity declined over time, although there was a slight resurgence of narrative alignment between PTI's official account and digital activists toward the end of the election period. The lower similarity scores among followers compared to core accounts can likely be partly attributed to the scale of data – tweets from 500 follower accounts naturally covered a broader range of topics, which reduces overall similarity.

Individual tweet comparisons further highlight differences in coordination between the two parties. PTI's official account and followers frequently posted extremely similar content, as reflected in numerous very high similarity scores, while PTI party leaders and the social media head showed slightly less narrative alignment with followers. In contrast, PML-N showed fewer extremely high similarity scores between core actors and followers, but the most glaring finding is the lack of narrative alignment between PML-N core accounts. Unlike PTI, very few tweets had extremely high similarity scores, indicating that the core accounts either posted about different topics or used different languages. Interestingly, for both PTI and PML-N, digital activists and friends showed no differences in narrative alignment with other actors.

Overall, PTI's messaging was more coordinated, with especially strong narrative alignment between its core accounts, while PML-N's communication appeared less coordinated. Core accounts from both parties initially aligned with digital activists, but this declined over time.

Content Dissemination and Coordination

To identify coordinated political campaigns, tweets were grouped based on similarity, and a clustering algorithm was used to detect patterns of organised messaging. Only clusters with significant activity and multiple actors were included to ensure meaningful results. Each cluster was manually reviewed to confirm coordination.

The four most prominent topics in coordinated campaigns were PTI, PML-N, the media, and foreign policy (see Figure 2.3). This reflects the overall most prominent topics during the election (see Figure 2.1). However, for coordinated campaigns, the political parties themselves were the most prominent topics. Both parties primarily made coordinated campaigns about their own party, which indicates that coordinated campaigns were primarily used to advance their own agenda. In the overall communication of political actors from both parties, the most prominent topic was foreign policy. However, in the coordinated campaigns, this topic is far less prominent. Notably, follower accounts engaged less on the topic of foreign policy and more on the political parties themselves. Thus, the most prominent topics in coordinated campaigns resembled the topics preferred by follower accounts more than the topics preferred by core accounts.

Follower accounts were the main contributors to coordinated campaigns (Figure 2.4a,c), while core accounts hardly contributed to these. This aligns

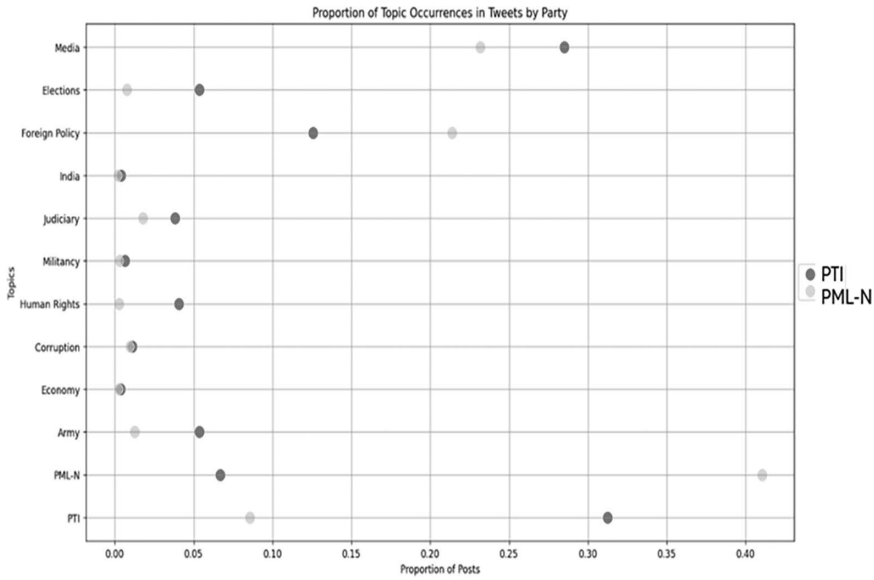


FIGURE 2.3 Plot showing the proportion of posts belonging to coordinated campaigns that relate to each of the topics from the previous section for PTI's coordinated campaigns and PML-N's coordinated campaigns, respectively.

well with the finding that the topics which most frequently occurred in coordinated campaigns were also those followers engaged in most. Surprisingly, the actors that contributed most to the coordinated campaigns were the friends, which had no explicit connection to the political parties. While friends were the most important actors in coordinated campaigns for both parties, digital activists played a bigger role in coordinated campaigns for PTI. This might indicate that PTI relied more heavily on followers with a direct connection to the party. Similarly, for both PTI and PML-N, the first tweet posted in most campaigns was made by a friend account. Some of the first tweets were also made by digital activists, and for PTI, the core accounts also initiated a small number of coordinated campaigns.

Overall, this indicates that the core accounts were not heavily engaged in coordinated activity and that this was instead relegated to follower accounts.

Conclusion and Discussion

Although traditional political actors still play a leading role in politics, this chapter provides empirical evidence that they are increasingly sharing space with new digital actors who play a central role in leading party communication and digital IO, even if they are not official members of a party. As

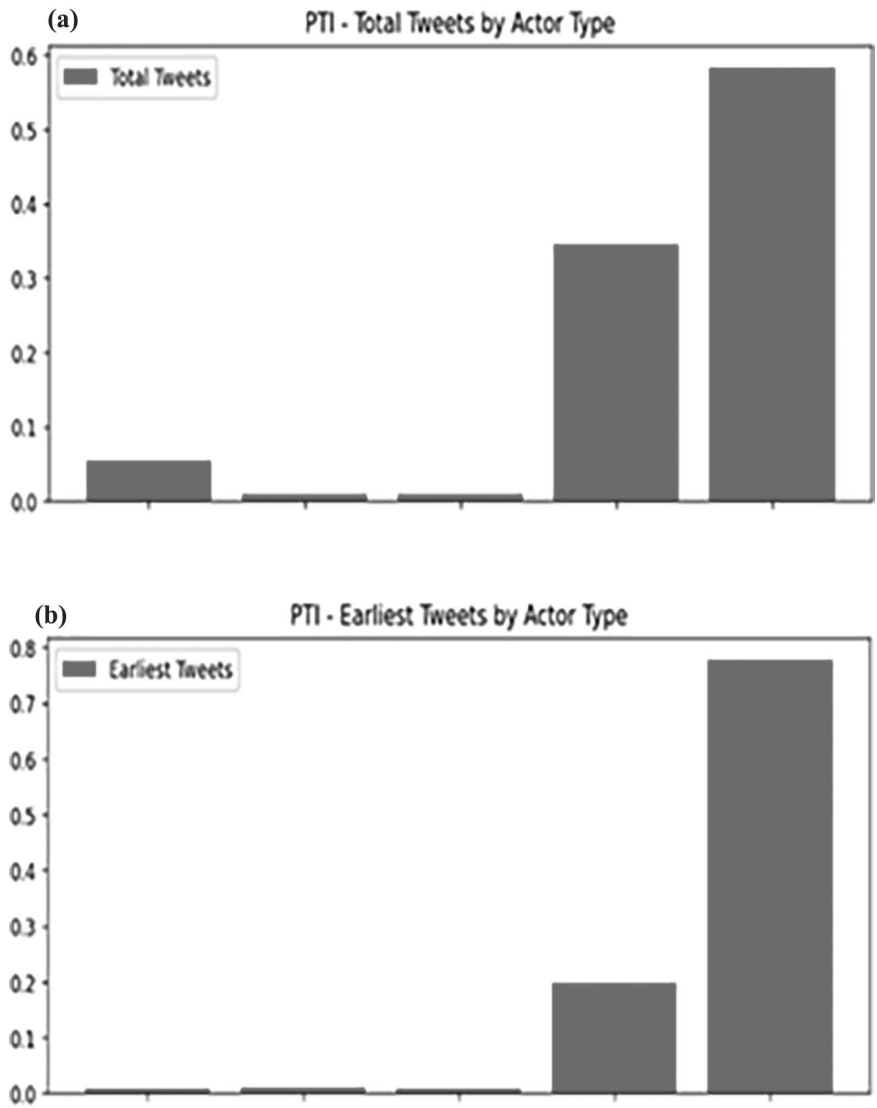
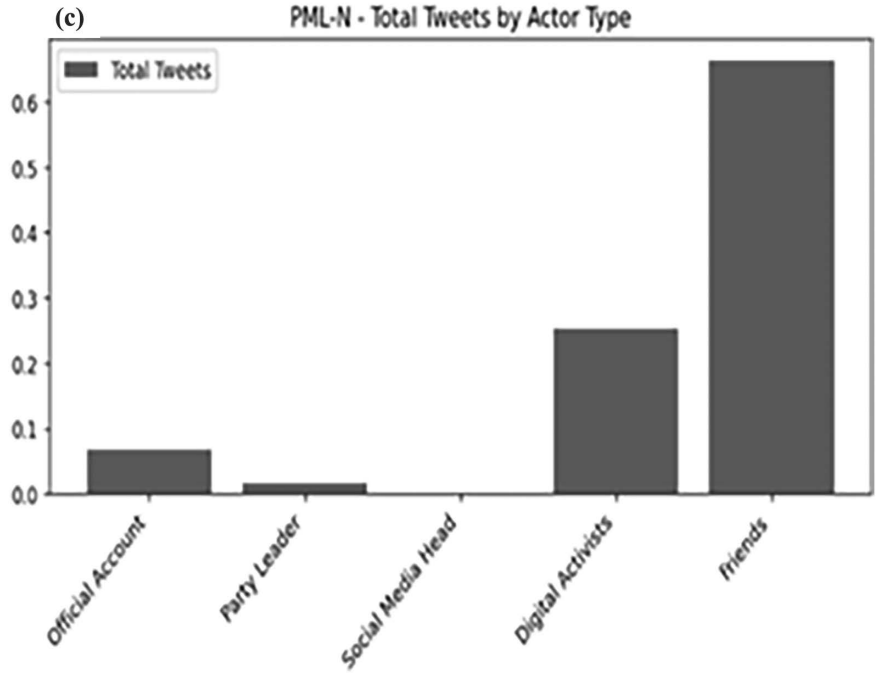


FIGURE 2.4 (a, c) Histograms indicating the proportion of actors involved in coordinated campaigns for PTI and PML-N, respectively. (b, d) Histograms showing the proportion of earliest posts in a coordinated campaign for each actor for PTI and PML-N, respectively.



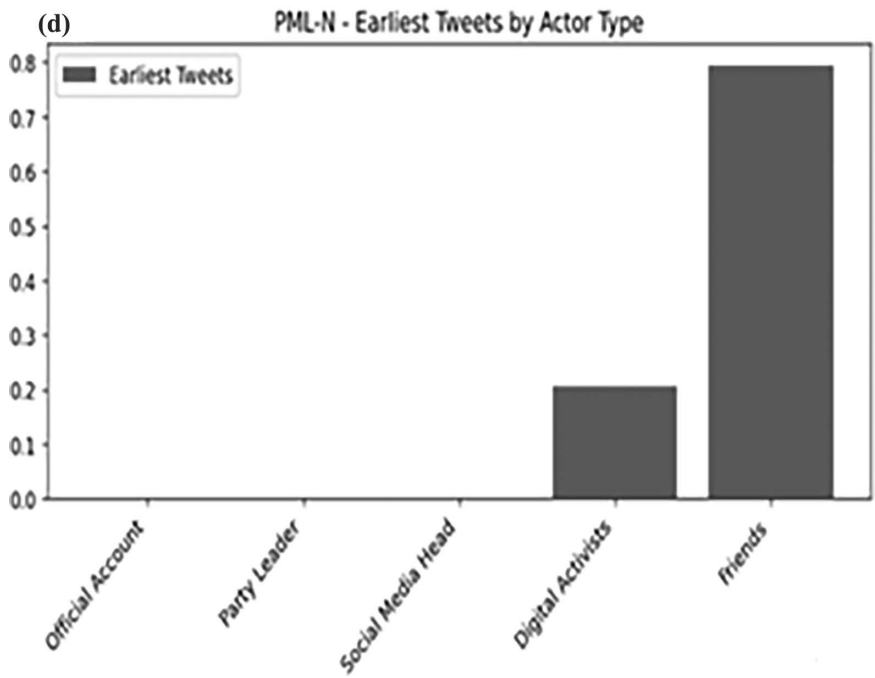


FIGURE 2.4 (Continued)

demonstrated through the coalitional framework proposed by Mir, Mitts, and Staniland (2023), there are direct and indirect ways through which non-electoral actors influence politics and align their content with political actors to help amplify party messaging. This study found that besides official party channels including party leaders, social media supporters (digital activists who visibly associate with a party in their Twitter bio, as well as party friends who do not visibly declare party support but still contribute frequently) play a central role in advancing party messaging, leading coordinated campaigns, and populating online discourse with a broader range of topics that align with the party narrative.

With more actors involved in party communication, party leaders are no longer the only source of electoral information or political campaigns. This is not unique to Pakistan but observed globally as discussed in other chapters on Nigeria, India, and Turkey. While previous studies suggest that party leaders talk about political topics more frequently than their supporters (Mir, Mitts, and Staniland 2023, 1344), this chapter found that official party channels no longer only include political leaders but that parties increasingly rely on their official Twitter pages as well as social media managers to discuss political topics of great importance, such as foreign policy. Therefore, we find that party social media leads, with their significant clout and strategic messaging, have become a central figure in traditional politics. Additionally, with parties investing in official social media teams over the years, supporter networks have also expanded significantly. A Washington Post investigation found that the ruling BJP in India had set up a sprawling apparatus of 150,000 social media workers to amplify its content across a network of WhatsApp groups (Shih 2023). Previous Pakistan elections witnessed more direct involvement of political leaders in party-focused messaging as well as coordinated campaigns on Twitter (Siddiqua 2021; Ahmed and Skoric 2014; Mulla 2017). In line with reporting on party supporter networks, this chapter found that political leaders were not actively involved in coordinated campaigns during the 2024 election and that these campaigns were party-centric and mainly led and run by party friends. These findings complement Abrahams and Leber's (2021, 1174) emphasis on "cyber knights" dominating the online sphere. Interestingly, friends do not visibly declare their party support, and yet they frequently contribute to political campaigns – further indicating the complexity of the digital political environment.

Not only do parties benefit from their supporter base for running promotional campaigns and posting in their favor, but these unofficial channels also allow discourse on topics that core actors may not directly engage on. Strikingly, while the army's interference in politics was not a major topic of conversation in the 2018 elections (Mir, Mitts, and Staniland 2023, 1344), this analysis provides evidence indicating that there was a discourse about the army around the 2024 elections. It's particularly interesting to note that it was the PTI's supporter networks who contributed to discussions about

the army. This finding not only highlights the role of non-electoral actors in evading state censorship and propagating discourse about controversial topics but also reflects the shift in PTI's political alignment since 2018 due to its fallout with the military. Interestingly, in 2018, human rights violations and concerns also found little space in the 2018 elections, and the topic was mostly central in dissident networks. This study found that PTI, despite being a mainstream party, posts about human rights online as part of its effective digital campaign against state censorship and political crackdown against the party and its leader Imran Khan.

Finally, I found the central role official Twitter pages of parties play in narrative alignment across actors. For instance, despite the overall lack of alignment between PML-N's core actors, we still find some similarities in content posted by PML-N's official Twitter account and its supporters. There was comparatively more similarity in content across the board for PTI; most actors had some overlap with the official Twitter account. This demonstrates that parties use their official social media channels to not only post party updates but also set the narrative to complement their offline politics.

Future research can help address the remaining gaps in this study. First, I did not use Urdu tweets for the full analysis. Second, we examined content on Twitter only, but with parties expanding their digital presence on other platforms such as TikTok and YouTube, these findings may not tell the full picture. Finally, the analysis of topics and campaigns relies on a relatively limited set of keywords and likely excludes many other topics the party actors engaged in.

Despite its limitations, this chapter reinforces the book's findings on the crucial role of non-electoral actors in digital operations. These endeavors have serious implications. Research cited here shows that party supporters not only amplify party messages but also spread cyber hate and target journalists, human rights defenders, and rivals – populist tactics inherent to SDIOs and observed in many political contexts explored in this book. While not always official party members, their scale and influence warrant further study into their motivations, shifting allegiances, and experiences as newcomers to traditional politics.

Appendix

Topics

"PTI": ["Imran", "PTI", "namanzoor", "Kaptaan", "bat", "IK"]
"PML-N": ["nawaz", "maryam", "pmln", "pml-n", "shehbaz", "sharif", "MNS", "sher"],
"Army": ["ispr", "fauj", "army", "establishment", "bajwa", "munir", "May 9", "Asim", "military"],

"Economy": ["economy", "inflation", "growth rate", "dollar"],
"Corruption": ["corruption", "Cipher", "nab", "Toshakhana"],
"Human Rights": ["censorship", "fascism", "human rights", "human right", "arrests", "jail"],
"Militancy": ["violence", "terror", "martyr", "militancy"],
"Judiciary": ["Isa", "chief justice", "court", "bandial", "faiz"],
"India": ["india", "modi", "kashmir"],
"Foreign Policy": ["america", "afghanistan", "saudi", "china", "Palestine", "TTP", "taliban"],
"Elections": ["rigging", "ECP", "protest", "independents", "results"],
"Media": ["TikTok", "Twitter", "X", "Facebook", "AI", "virtual", "social media", "blackout", "TV", "mainstream"].

References

Abrahams, A., and A. Leber. 2021. "Comparative Approaches to Mis/Disinformation| Electronic Armies or Cyber Knights? The Sources of Pro-Authoritarian Discourse on Middle East Twitter." *International Journal of Communication* 15: 27.

Afzal, M. 2024. "Pakistan's Surprising and Marred 2024 Election, and What Comes Next." *Brookings*, February 6. https://www.brookings.edu/articles/pakistans-surprising-and-marred-2024-election-and-what-comes-next.

Ahmed, S., K. Jaidka, and J. Cho. 2016. "The 2014 Indian Elections on Twitter: A Comparison of Campaign Strategies of Political Parties." *Telematics and Informatics* 33 (4): 1071–87. https://doi.org/10.1016/j.tele.2016.03.002.

Ahmed, S., and M. M. Skoric. 2014. "My Name Is Khan: The Use of Twitter in the Campaign for 2013 Pakistan General Election." In *2014 47th Hawaii International Conference on System Sciences*, 2242–51. Waikoloa, HI: IEEE. https://doi.org/10.1109/HICSS.2014.282.

Batool, S. H., W. Ahmed, K. Mahmood, and H. Saeed. 2022. "Twitter Dialogue: An Analysis of Pakistani Politicians' Information Sharing." *Information Discovery and Delivery* 50 (1): 64–74. https://doi.org/10.1108/IDD-03-2020-0031.

Borucki, I., and J. Fitzpatrick. 2021. "Tactical Web Use in Bumpy Times – A Comparison of Conservative Parties' Digital Presence." In *Digital Parties: The Challenges of Online Organisation and Participation*, edited by O. Barberà, G. Sandri, P. Correa, and J. Rodríguez-Teruel, 245–67. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-78668-7_13.

Bradshaw, S., H. Bailey, and P. N. Howard. 2021. *Industrialized Disinformation 2020 Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute.

Bradshaw, S., and P. N. Howard. 2018. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71 (1.5): 23–32.

Cheema, H. 2020. "War, Lies and Hashtags: Pakistan's Twitter Battles." *Al-Jazeera*.

Chhibber, P. K., and S. L. Ostermann. 2014. "The BJP's Fragile Mandate: Modi and Vote Mobilizers in the 2014 General Elections." *Studies in Indian Politics* 2 (2): 137–51. https://doi.org/10.1177/2321023014551870.

Curran, E., and A. Crawford. 2023. "Brace for Elections: 40 Countries Are Voting in 2024." *Bloomberg*, November 1. https://www.bloomberg.com/news/articles/2023-11-01/brace-for-elections-40-countries-are-voting-in-2024.

Dutt, B. 2024. "Ideas | How Narendra Modi Became India's Influencer-in-Chief." *Rest of World*, February 13. https://restofworld.org/2024/narendra-modi-youtube-influencer/.

Fahmy, S. S. 2017. "Media, Terrorism, and Society: Perspectives and Trends in the Digital Age." *Mass Communication and Society* 20 (6): 735–39. https://doi.org/10.1080/15205436.2017.1382285.

Freelon, D., and C. Wells. 2020. "Disinformation as Political Communication." *Political Communication* 37 (2): 145–56. https://doi.org/10.1080/10584609.2020.1723755.

Gibson, R., F. Greffet, and M. Cantijoch. 2017. "Friend or Foe? Digital Technologies and the Changing Nature of Party Membership." *Political Communication* 34 (1): 89–111. https://doi.org/10.1080/10584609.2016.1221011.

Gohdes, A. R. 2020. "Repression Technology: Internet Accessibility and State Violence." *American Journal of Political Science* 64 (3): 488–503.

Howard, P. N., and B. Kollanyi. 2016. "Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2798311.

Hussain, S., F. Shahzad, and A. Saud. 2021. "Analyzing the State of Digital Information Warfare Between India and Pakistan on Twittersphere." *SAGE Open* 11 (3): 215824402110319. https://doi.org/10.1177/21582440211031905.

Jahangir, R. 2020. "Life in Pti's Social Media Bubble." *DAWN.COM*, August 16. https://www.dawn.com/news/1574529/life-in-ptis-social-media-bubble.

Jahangir, R. 2021. "Pro-Government 'Fact Checkers' Are Vilifying Pakistani Journalists." *Coda Story*, May 28. https://www.codastory.com/authoritarian-tech/pakistan-harassment-journalists/.

Jahangir, R. 2022. "Riding the Social Media Tiger." *DAWN.COM*, June 5. https://www.dawn.com/news/1693238/riding-the-social-media-tiger.

Jahangir, R. 2023. "Imran Khan is fighting Pakistan's Army with Twitter." *Coda Story*, May 25.

Jorgic, D., and A. Pal. 2019. "Facebook, Twitter Sucked into India-Pakistan Information War." *Reuters*.

Lobera, J., and M. Portos. 2021. "Decentralizing Electoral Campaigns? New-Old Parties, Grassroots and Digital Activism." *Information, Communication & Society* 24 (10): 1419–40. https://doi.org/10.1080/1369118X.2020.1749697.

Mir, A., T. Mitts, and P. Staniland. 2023. "Political Coalitions and Social Media: Evidence from Pakistan." *Perspectives on Politics* 21 (4): 1337–56. https://doi.org/10.1017/S1537592722001931.

Mir, A., and T. Salikuddin. 2024. "Understanding Pakistan's Election Results." *United States Institute of Peace*, February 13. https://www.usip.org/publications/2024/02/understanding-pakistans-election-results.

Mufti, M., S. Shafqat, and N. Siddiqui. 2020. *Pakistan's Political Parties: Surviving between Dictatorship and Democracy*. Georgetown University Press.

Mulla, A. 2017. "Mediatized Populisms| Broadcasting the Dharna: Mediating 'Contained' Populism in Contemporary Pakistan." *International Journal of Communication* 11 (0): 16.

Munger, K., R. Bonneau, J. Nagler, and J. A. Tucker. 2019. "Elites Tweet to Get Feet Off the Streets: Measuring Regime Social Media Strategies During Protest." *Political Science Research and Methods* 7 (04): 815–34. https://doi.org/10.1017/psrm.2018.3.

Schliebs, M., H. Bailey, J. Bright, and P. N. Howard. 2021. "China's Public Diplomacy Operations: Understanding Engagement and Inauthentic Amplifications of PRC Diplomats on Facebook and Twitter." *DemTech Working Paper*. Programme on Democracy and Technology, Oxford University.

Shih, G. 2023. "Inside the Vast Digital Campaign by Hindu Nationalists to Inflame India." *Washington Post*, September 27. https://www.washingtonpost.com/world/2023/09/26/hindu-nationalist-social-media-hate-campaign/.

Siddiqua, A. 2021. "Use of Cyber Hate in the Electoral Campaigns by the Mainstream Political Parties of Pakistan." *Humanities & Social Sciences Reviews* 9 (2): 325–32. https://doi.org/10.18510/hssr.2021.9232.

Singh, K. 2024. "US, UK and EU Urge Probe into Pakistan Election, Express Concerns." *Reuters*, February 10. https://www.reuters.com/world/us-uk-eu-urge-probe-into-pakistan-election-express-concerns-2024-02-09.

Sinha, A. 2023. "Regulating Diffuse Actors in the 2024 Indian Elections." *The Influence Industry Project*. https://influenceindustry.org/en/explorer/case-studies/india-sinha-diffuse-actors/.

Tshuma, B. B., L. A. Tshuma, and M. Ndlovu. 2022. "Twitter and Political Discourses: How Supporters of Zimbabwe's Ruling ZANU PF Party Use Twitter for Political Engagement." *Journal of Eastern African Studies* 16 (2): 269–88. https://doi.org/10.1080/17531055.2022.2076385.

Yilmaz, I., R. M. A. Saleem, M. Pargoo, S. Shukri, I. Ismail, and K. Shakil. 2022. "Religious Populism, Cyberspace and Digital Authoritarianism in Asia: India, Indonesia, Malaysia, Pakistan, and Turkey." *Deakin University*. https://hdl.handle.net/10536/DRO/DU:30162438.

3

DIS/MISINFORMATION, VISIBILITY POLITICS, POPULISM, AND DIGITAL INFORMATION

An Analysis of Pre- and Post-2023 Nigerian General Elections

Najimdeen Ayoola Bakare

Introduction

For many Nigerians, the return of democracy in 1999 marked a turning point after a long history of military regimes. Since 1999, Nigeria has conducted numerous elections, positioning the country as one of the African nations with fairly managed democratic credentials. Even with such political credentials, critics still consider the Nigerian political architecture as illiberal. The 2023 general elections marked a significant watershed in the nation's political evolution, leaving an indelible mark in its political history. Leading up to the 2023 general elections, the Nigerian political terrain was highly charged, with various competing views vying for political visibility and prominence in the marketplace of public opinion. Social media platforms played a pivotal role in this competition. The period before and after the elections witnessed an extensive use of digital media technologies, primarily aimed at engaging in the politics of visibility. This was characterised by significant youth political activism, with a strong emphasis on challenging existing power structures.

As it is with elections worldwide, electioneering seasons often witness political campaigns that can be tumultuous, rancorous, and occasionally violent. Such conflictual behaviors do not occur in isolation; instead, they are incentivised by various competing factors. The rapidity, proliferation, and intensity of information, especially in the digital age, have significantly contributed to the evolution of elections worldwide. While digital information offers numerous benefits, it is not immune to shortcomings, which arise as a result of its application.

Digital information encompasses various descriptions, with one prominent aspect being the internet and its associated platforms, such as social

DOI: 10.4324/9781003628088-4
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

media. Politics in the internet age has transcended the physicality of the public sphere. Political visibility, the expansion of political geography, persuasion of electorates, and criticism of political opponents now predominantly occur through digital information on cyber platforms. Interestingly, these platforms facilitate the phenomenon of "post-truth," which challenges the established regime of truth (Arif and Bakare 2022).

This chapter elucidates the instrumental role of digital (dis)information in the Nigerian polity. It seeks not only to understand but also to demonstrate how (dis)information contributes to the politics of visibility before, during, and after the 2023 Nigerian general elections. Unlike previous elections, particularly those in 2015 and 2019, the 2023 elections showcased the extent to which ethno-religious political sentiments were publicly celebrated and fervently embraced, often at the expense of national unity. In this context, the chapter explores how (dis)information via digital platforms marked a significant turning point in the nation's political evolution, leaving an indelible mark on its political history. Additionally, the chapter examines how digital information facilitated digital populism, which I define as a situation where a politician gains political traction and a large following through (dis)information, especially among the youth and middle class, who are active users of digital platforms (Federal Ministry of Youth and Sports Development 2020), especially the social media spaces. Ninety-five percent of Nigerian youth can surf the internet – given its availability, accessibility, and affordability in a country punctuated by the proliferation of affordable android smartphones (Guardian 2021).

To provide context and conceptual analysis, the chapter employs "visibility politics," investigating the intersection of (dis)information, digital information, and identity politics. Leading up to the 2023 general elections, the Nigerian political terrain was highly charged, with various competing views vying for dominance and prominence in the public opinion marketplace. Social media platforms played a pivotal role in this competition. Before and after the elections, there was extensive use of digital media technologies, primarily aimed at engaging in the politics of visibility. This was characterised by significant youth political activism, with a strong emphasis on challenging existing power structures. Setting the tone with "visibility politics" as a conceptual framework in the first section allows for the examination of five critical objectives: (1) How was (dis)information and (mis)information strategically used as part of identity politics and the politics of visibility? (2) to analyze the strategic manipulation of digital media to influence election outcomes, including attempts at pre-election rigging well in advance of the election days; (3) to examine how digital information was employed to generate and propagate conspiracy theories against opposing political parties, ultimately advancing a populist agenda in support of a particular political figure who garnered significant appeal among the youth population; (4)

to explore how digital media exacerbated ethno-religious politics, deepening political polarisation, fostering ethnic and religious tensions, and even fueling calls for secession; and (5) to analyze the implications of digital media in the resurgence of spatial nationalism – convergence of political actors both within and among the diaspora.

Conceptual Consideration – Visibility and Identity Politics

The chapter draws upon sociological insights into the concept of "visibility politics," considering its multifaceted contextual utility. Interestingly, scholarship has shown the intersection of visibility politics, identity politics, and power relations (Brighenti 2007; Creech 2020; Rega and Medrado 2023; Whittier 2018). Visibility politics manifests as a quest for power, recognition, and contestation within social (public) spaces. In Foucauldian terms, power transcends mere influence, encompassing the challenge of power by understanding the tools and techniques through which it operates. Foucault (1979) notes,

> power works through modes of knowledge and visibility as both a type of control and as a counterpoint to that control, and thus capturing the apparatuses of visibility also opens up the possibility of affecting the relations of power that produce and are produced.

In the Nigerian context, one may argue that the Nigerian youth not only comprehend digital technologies and knowledge production techniques but also master them, enabling them to politically challenge and contest the dominant political narrative/knowledge. In doing so, they politically produce visibility for themselves. Jiménez-Martínez and Edwards (2023) observe that most social movements employ communicative efforts not merely to challenge dominant social arrangements but as a means of "acquiring, maintaining, and/or managing visibility is indispensable" and "managing visibility is indispensable" (Jiménez-Martínez 2021; Neumayer and Rossi 2018; Uldam 2018). Visibility politics implicates and exposes power relations, as power associated with visibility is prone to asymmetry – "asymmetries and distortions of visibility are the norm" (Brighenti 2007). The political visibility conferred upon Nigerian youth by the internet technologies can easily result in power matrix or (in)visibility asymmetries, thereby making them vulnerable to surveillance (Rega and Medrado 2023).

A significant body of scholarship has demonstrated the nexus of power, surveillance, discipline, and punishment (Bucher 2012; De Backer 2019; Foucault 1977), especially in the internet age. Politics of visibility is an all-inclusive venture, requiring individual and collective consciousness and rallying around a common shared value or goal. For Whittier (2018),

"Identity politics" organise people around a collective identity, while identity visibility is the goal. Similarly, at the core of identity politics are visibility tactics, the propensity for making collective identity visible (Whittier 2009), serving as a channel for identity recruitment and solidarity (Whittier 2018), and avenue for social exclusion and marginalisation (Brighenti 2010; Uldam 2018). Collective identities may be politicised through power struggles as groups define their shared grievances, assign blame for their position, and call for action (Klandermans 2014; Taylor and Whittier 1992). To maintain and sustain result-oriented visibility, actors vying for visibility must embrace and promote some form of visibility strategies, which are a "central component for the maintenance, subversion, and reconfiguration of power relations" (Jiménez-Martínez and Edwards 2023, 6). An important element of group identity is identity strategies, which involve "coming out," a key component of visibility politics according to Whittier (2009). Identity strategies may purposefully critique existing definitions (Bernstein 2005) and produce change to ensure the security of a group's collective identity and the public visibility of the group's worldview. Besides, these strategies manifest in various ways, one of which is the variety of internet platforms, as discussed in the following sections of this chapter.

(Dis)information and (Mis)information, and Identity and Visibility Politics

The relationship between post-truth and (dis)information and (mis)information has been well studied (Ball 2017; D'Ancona 2017; Davis 2017; Farkas and Schou 2020; Foroughi, Gabriel, and Fotaki 2019; Ghosh 2022), especially in a dynamic cybersphere characterised by social media platforms (Hazzan 2023). While the connection between electioneering and media is not new, it has garnered enormous attention in an era of social media proliferation, leading to expansive, intense, and extensive political participation, which may not necessarily equate to being well informed but rather to ill awareness. Combined with the use of digital media for electioneering purposes, the period before and after the 2023 Nigerian general elections was marked by an identity crisis and politics of visibility. With the help of digital technologies, social media platforms became spaces for contesting political visibility. The visibility phenomenon did not merely serve as evidence of social and political conditions but also invariably created the ideological realm where power relations are envisioned, expressed, and taught (Creech 2020).

The mass utility of digital technologies underscores the power of Nigerian youth. It has shown the degree to which youth can challenge the status quo. For instance, using different social media platforms, Nigerian youth disrupted the course of affairs, as state power to dominate and decide the trajectory of

information was not only obstructed but also contested. This phenomenon of power relations exemplifies what Creech (2020) terms as the politics of visibility. Using digital technologies to challenge the powers-that-be took a new turn prior to the 2023 general elections. Thus, echoing Berger: "If the new language of images were used differently, it would . . . confer a new kind of power. Within it, we could begin to define our experiences more precisely" (Berger 1972, 33). In fact, the reality generated by digital technologies in Nigerian politics surpasses mere political socialisation or broad political participation; it embodies a space that reveals the relationship between power relations and mass culture (pop culture) – online politicking. The contest further exposed the generational gap between old and emerging political players. For instance, in the case of Nigeria, the use of social media for electioneering purposes allows for youth visibility, demonstrating the maturity of Nigerian politics beyond the physicality of the public sphere. It also underscores the readiness of youth to not only make themselves politically visible but also prove their political enthusiasm, assertiveness, and how much they want to be a part of determining the political future of the country. This action does not fall short of visibility; in fact, the desire to be pragmatic and the quest for political recognition and control exemplified using digital technologies and spaces for acquiring visibility. In doing so, the actions of Nigerian youth reckon with the contextual understanding of visibility as a condition for recognition (Brighenti 2007) and equally a means of control (Rega and Medrado 2023).

Political visibility and identity crisis may face challenges in an era where (dis)information and (mis)information abound. For instance, Peter Obi, the presidential candidate for the Labour Party (LP), has gained significant visibility on social media through his supporters. Besides positioning himself as a populist leader wanting to liberate the Nigerian masses from the clutches of the elites, his claim of being a clean politician failed to be insulated from online posts targeting him as a sectionalist and religious bigot (Salako 2023). Such labeling was used by his opponents to discredit him, targeting his political visibility. Similarly, among all the presidential candidates in the 2023 general elections, President Ahmed Bola Tinubu led the race in a visibility crisis. Another way to expound on visibility and identity politics is how the Nigerian sociopolitical terrain heated up.

For instance, long before the 2023 elections, religion and ethno-tribal sentiments have always had significant influence on the polity, but the 2023 elections took a new turn as religious institutions, especially the Church (Akinkuotu 2022), noticeably steered divisive political narratives, openly weaponised religion and endorsed Peter Obi's candidacy, "Pastors of mega churches in Nigeria are donating their church auditoriums for the registration of voters, while making sermons that point to their heart's desire to see Peter Obi become the president of Nigeria" (Phillips 2022). The Church

narratives were not insulated from (dis)information and (mis)information used in the galvanisation of their members. The romance between Obi and the Church exemplified identity politics and visibility, while reinforcing how collective identity – either of religion or ethnicity is vulnerable to politicisation and instrumentalised in defining shared grievances and seeking relevance in a contest public (political) space.

Digital Media Strategic Manipulation and Influence on Elections

Whether true or false, the claim that politics is a dirty game becomes even dirtier amid the proliferation of unverifiable information on different social media platforms and other internet outlets. Like in many cases, digital media has increasingly been pivotal in impacting election outcomes. A vivid and relevant reference case is the outcome of the 2016 American elections, which led to the victory of President Trump. Russia's interference in American domestic politics through digital media manipulation is said to have contributed to the defeat of Hillary Clinton and the victory of President Trump (Allison et al. 2017; Harding, Borger, and Sabbagh 2021; Mayer 2018).

First, in the case of Nigeria, the pre-2023 general elections politicking and activism are closer to being considered as avenues to effect change and were used to generate a collective identity among those who dislike the past, scorn the present, and desire a better future for Nigeria. Indeed, the politicisation of collective identity was carefully engineered to promote participation in political protests against the establishment (van Stekelenburg 2013). Second, in the case of Nigeria, media contents during the electioneering days were not just toxic but epitomised (dis)information and (mis)information. For instance, to denigrate and disparage the candidacy of President Ahmed Bola Tinubu, social media platforms such as X–Twitter were punctuated with barrels of trending hashtags such as #BolaTinubuCommittedPerjury, #TinubuTheDrugDealer, #BolaTinubuIsDrugDealer, #TinubuTheDrugLord, #TinubuForPrison, #Tinubu4Prison, and #TinubuIsAConvictedDrugDealer. These hashtags were crafted to further disgrace his All Progressive Congress (APC), which was already condemned by many Nigerians for bad governance under the Buhari presidency. Associating illicit drug ventures and perjury with Tinubu was a form of political and character assassination, while clearing the way for Peter Obi (#PeterObi4President2023) as a clean politician who could be voted for as president of Nigeria. A similar degrading hashtag was launched against Dr. Rabiu Kwankwaso, the presidential candidate of the New Nigerian Peoples Party (NNPP). The debate generated tends to misinform the truth about Kwankwaso's academic degree (PhD in Water Engineering). For his supporters, such misinformation was smear tactics and amounted to clustering him among politicians and public officers accused of certificate forgery. Based on its fact-check exercise, the Centre for Democracy and Development (CDD-West Africa) investigated the

#KwankwasoFakeResult and eventually cleared him of the misinformation.[1] The nexus of digital media and elections in Nigeria has never been a novel phenomenon; studies show the relationship in the 2015 Nigerian general elections, but the phenomenon attained height in the 2023 elections due to multiple competing reasons such as religiosity, ethno-tribalism, the availability and accessibility of the internet, heightened economic dislocation, and generational dissonance, among others.

To influence election outcomes, the three major presidential candidates – Peter Obi, Atiku Abubakar, and Bola Ahmed Tinubu – increased their followership on Facebook and X–Twitter. Daily, these platforms got littered with hashtags directly related to candidates. As the online political followership underscores the significance of social media in electoral politics in Nigeria, it equally demonstrates the political restlessness among voters to ensure that their candidates make it to the presidency. Meanwhile, the fruition of such aims may not necessarily exclude the use of (dis)information, (mis)information, and social media bots, and numerous websites disseminate false stories to attract and gather a huge readership (Nwonwu, Tukur, and Alo 2023). Commenting on the political trend leading to the 2023 elections, Tobi Oluwatola reiterated electoral manipulation and (mis)information, particularly in an age of advanced digital media, for which "candidates always use false information to discredit their opponents and embellish their records, with or without veracity. Incidents of these are already rife in the political space" (Luckscheiter 2022). Oluwatola further stressed the link between false information, false representation (through bots), and electoral processes.

> Popular hashtags related to the major political candidates of the 2023 general elections revealed bot operations. Hashtags such as #BATified, #Obidient, #Atikulated, #kwankwasiya, etc. were found to have been driven by bots. This camouflaged scheme is likely to intensify as the elections draw closer . . . These bots are able to trend any topic quickly and create an illusion of a movement out of what may be a fringe view.
>
> *(Luckscheiter 2022)*

Supporting Oluwatola's argument, Mayowa Tijani asserts that the proliferation of deep fakes and fake websites has clearly impacted the national discourse, as narratives embraced by such websites often become national conversations. He further emphasises,

> Now, when one of them comes up with a false story, there is a high chance that other websites will pick it up, making it very influential on social media. They help push it further, and it spreads offline, becoming the dominant narrative.
>
> *(Nwonwu, Tukur, and Alo 2023)*

Being one of the most widely used social media platforms for political discourse, X–Twitter Spaces, launched by the media giant, provided a platform for open and unfiltered conversations. However, these spaces also contributed to the amplification of misinformation and disinformation. The following comments by Aisha Ibrahim Abba further illuminate the issue:

> This is worrying because Twitter Spaces are hosted by individuals who, most of the time, have preempted intentions as to why they are hosting the Space. Moreover, some of the speakers in these spaces are not experts per se, but rather people who would gather mass followership.
>
> *(Garba 2023)*

The strategic manipulation of digital media to influence election outcomes, including pre-election rigging, does not solely rely on the use of bots and fake websites as primary enablers of manipulation. In fact, (dis)information and (mis)information combine the virtual and actual machinations of paid and unpaid political influencers both online and offline. In the case of the 2023 elections, these influencers propagated (dis)information and (mis)information favorable to their preferred candidates while targeting and damaging the image of their opponents. For instance, X–Twitter hashtags such as #BolaTinubuCommittedPerjury, #TinubuTheDrugDealer, #BolaTinubuIsDrugDealer, #TinubuTheDrugLord, #TinubuForPrison, #Tinubu4Prison, and #TinubuIsAConvictedDrugDealer are good reference points. Additionally, instances of "deep fakes" – where AI-doctored images and videos purported to mislead and generate negative narratives – were identified during the 2023 elections.

One of the key takeaways from the election is how distinct modes of visibility are produced by power in order to control society (Gordon 2002), albeit in this context, through social media. The machinations of digital technologies reinforce Foucault's contribution to our understanding of power, indicating that power transcends mere influence and also involves challenging power by mastering the tools, machinery, and techniques used by power. Foucault notes,

> power works through modes of knowledge and visibility as both a type of control and as a counterpoint to that control, and thus capturing the apparatuses of visibility also opens up the possibility of affecting the relations of power that produce and are produced.
>
> *(Foucault 1979)*

Nigerian youth, especially those who believe in challenging and changing the political establishment and structure, have learned to make themselves more politically visible through the mastery of digital technologies, thereby altering power dynamics.

The amount of (dis)information and (mis)information disseminated on Nigerian social media platforms did not dissipate or end with the culmination of the elections; instead, it carried over into the post-election environment. For instance, days after the inauguration of President Ahmed Bola Tinubu as the 43rd Nigerian president, some Nigerians utilised social media to denounce Tinubu as their president with X–Twitter hashtags such as #TinubuIsnotMyPresident, #NotMyPresident, #TinubuDidNotWinAnyElection, and #TinubuMUSTbeDisqualified. These social media posts were crafted not only to denounce Tinubu's presidency but also to reject the "claimed rigged elections" by the Independent Election Commission (INEC), the body responsible for managing elections in Nigeria, and to underscore the candidacy of Labour Party (LP) candidate Peter Obi, who some believed had won the election but lost due to INEC manipulation (Alabi 2023). Post-election periods in Nigeria often lack political serenity and are instead characterised as an extension of the political acrimony that punctuated the electioneering period. The victory of President Tinubu was unacceptable to many Obidient (the political tag for Peter Obi and Yusuf Datti's supporters) who had presumed their presidential candidate would be declared the winner. This disappointment heightened the online battle between the BATified and Obidient factions, leading to hashtags such as #TinubuIsACertificateForger, #TinubuMustBeDisqualifiedNow, #AllEyesOnTheJudiciary, and #TinubuMustResign, especially as the economic situation worsens.

Digital Media, Ethno-Religious Politics, Populism, Secessionism

The election exacerbated an already precarious ethno-tribal and religiously charged political environment. The use of social media and the attendant misinformation deepened political polarisation, fostered ethno-religious tensions, and at worst, helped inflame the controversial agitation for secession (Bakare 2021, 2024). The foremost presidential candidates – Peter Obi, Atiku Abubakar, Bola Ahmed Tinubu, and Rabiu Kwankwaso – could not escape being painted with ethno-religious colors. Among all the presidential contestants, Peter Obi was closer to adopting populist rhetoric. The accessibility, ubiquity, and availability of the internet enabled what I define as digital populism. Digital populism, as I define it, is a situation where an individual or politician gains political attention and a large following through (dis)information, especially among the youth and middle class, who happen to be active users of many digital platforms. Digital populism is a non-ideologically driven form of populism. The digital populist enjoys a free ride due to unimaginable online support and, like other forms of populism, it exploits and preys on the aggrieved sentiments of the public toward the elites, structures, and institutions believed to be non-people-centric. Digital populism goes beyond "performative activism" (Jiménez-Martínez and

Edwards 2023); it exposes the vulnerability of the Nigerian polity to political acrimony – a kind that transcends the physicality of the public sphere to the virtual space of cyber sphere.

Positioning himself as a populist leader, Peter Obi exploited the generational dissonance that has built up over a period between the youth and the old elites. He called on the youth, stating, "It's time to take your country back" and framed the election as "the old against the new" (Ndubuisi and Orjinmo 2023). Obi's stance on rallying youth votes was made unequivocal during his speech at Chatham House, where he declared, "Nigeria today is at a critical juncture, and the people, led by the youths brutalised by bad leadership, are awake and leading the movement to transform Nigerian politics" (Mureithi 2023). His stance may explain the positive sentiment toward him, especially on X–Twitter – "Peter Obi has more favorite words as well as more positive favorite words than either of his peers – other contesting for the presidency" (Olabanjo et al. 2023, 7), aligning with the social media content (#PeterObi4President2023) associated with his supporters. As a non-ideological populist, Peter Obi made significant headway in terms of X–Twitter impressions and engagements compared to other contenders for the presidency (Olabanjo et al. 2023).

Given his populist rhetoric, it was presumably believed that the Nigerian youth were sympathetic and supportive of Peter Obi's candidacy (Mureithi 2023). Many also considered him as largely supported by Nigerians of Igbo extraction from the Eastern part of the country and simultaneously as a candidate for Nigerian Christians who openly expressed their preference for Obi, while vehemently opposing any Muslim candidate at the polls (Casper 2023; Ndubuisi and Orjinmo 2023). Obi himself also weaponised religion, utilising the platforms of the Nigerian church. His indelible speeches "Church, wake up. Take back your country" (Opejobi 2023) – "Yes daddy, this is a religious war" (The Cable 2023) underscore the weaponisation of religion. Similar weaponisation of religion can be said of other candidates, especially Atiku Abubakar of the Peoples Democratic Party, Rabiu Kwankwaso of NNPP, and Bola Ahmed Tinubu of APC, who are Muslims and were viewed as the Muslim candidates from the north and southwest, respectively.

Most studies on the nexus of social media/digital technologies and electoral politics are often tempted to underscore the negative impacts of the link, while paying less attention to its constructive and critical dimension. Constructively, on account of the social media/digital technologies, the 2023 general elections exposed the embedded fault lines in Nigerian political architecture. It equally unveiled the paradoxically utility of social media and digital technologies. While Peter Obi galvanised a *persuasive yet "dangerous" populist agenda,* commanded a sizable public support from within and outside Nigeria, as a result of misinformation and disinformation, social media

representation of him, unveiled the paradox of his non-ideological populism. In a similar vein, Obi could not escape being labeled as regionalist, despite the effort to pitch and portray himself as a Nigerian – nationalist, segment of the social media saw him through the lens of ethnicity, tribal politics, and sectionalism (Ndubuisi and Orjinmo 2023). This became more telling, especially when media report shows that sizable supporters of his electoral campaign were from the Eastern region of Nigeria, the same region of origin of Peter Obi (Busari 2022). More interestingly, the social media electioneering process sharply underlined what Ebenezer Obadare refers to as the "ethnic impulse" – the conviction of the Igbo that "it is our turn" to produce the next Nigerian president (Obadare 2023). The Igbo have long carried the baggage of the Nigerian Civil War and the disdain of being considered illegitimate for the presidency.

Interestingly, Nigerian politics is such a complex game that the success of any presidential candidate is contingent on the collective votes of Muslim and Christian voters, regardless of their tribe or ethnicity. Second, even when Peter Obi was labeled as the candidate of the Nigerian Church, his running mate – vice president of the Labour Party (LP), Yusuf Datti Baba-Ahmed – is a Muslim. Though unwritten, religion and tribe decide who stands for the position of president and vice president. While the Nigerian constitution is silent on the matter, the long tradition and practice suggest that the two offices of the president and vice president should not be filled by persons from the same faith or tribe, although Nigerian political history has fewer exceptional cases not in tangent with such tradition. For instance, during the 2023 elections, APC campaigned and won on a same-faith (Muslim–Muslim) ticket, where the president and vice president were from different ethnic extractions but shared the same faith, is the most recent example. Third, given the primordial trajectory of the election period, the Nigerian political terrain failed to escape its perennial nemesis of one part of the federation wanting to separate. The candidacy of Peter Obi transcends his religious affiliation; being an Igbo in the presidential race boosted the morale of the Igbos, who make up the country's third-largest ethnic group. The Igbos have always claimed political marginalisation and victimisation. Since independence, the country has never had an Igbo hold the position of president, save President Nnamdi Azikwe, an Igbo, who was the first ceremonial Nigerian governor general and president after independence in 1960. Peter Obi's candidacy also generates online debate, as to whether the Indigenous People of Biafra (IPOB) – a separatist and terrorist Igbo group – offers him support (Nwonwu, Tukur, and Alo 2023), although his X account shows his dislike for criminality of the group in the Southeast of the country.[2] IPOB wants to revive the Biafra Republic as a separate political entity from the Nigerian Federation. The Biafra Republic was created and spearheaded by the Igbo during the Nigerian Civil War between 1966 and 1969.

Digital Media, Spatial Nationalism, and Diaspora Political Participation

While it remains undisputed how evolving social media platforms have enabled collective identity visibility (Whittier 2009), fostering solidarity across social movements and classes, serving as platforms for identity recruitment (Whittier 2018), and providing an avenue for creating experiential visibility that draws geographically disparate individuals into the intimate sociality of various social movement projects (Thorburn 2014), it is also undeniable that these same platforms have contributed to contestation, social exclusion, and marginalisation in terms of visibility (Brighenti 2010; Uldam 2018). In all of these characterisations, digital media has also uniquely fostered an experiential visibility that is transnational. Hence, in the case of Nigeria, experiential visibility and political socialisation not only are confined to domestic players but also include the Nigerian diaspora dispersed around the world. In this context, I argue that digital media is increasingly stimulating spatial transnationalism. Transnationalism is understood as the social process migrants use to link the social spaces of their countries of origin and settlement, a process involving the exchange and flow of information and conversation (Kurtenbach 2017; Schiller, Basch, and Blanc-Szanton 1992), especially in an era of the democratisation of digital technologies and the availability of handy technological devices (smartphones, laptops) and platforms (Skype, Facebook, and X–Twitter). What distinguishes spatial transnationalism from transnationalism is the fact that the former takes into account the prevailing situations in the home country – the country of origin. Migrants or the diaspora desire to see the realisation of better governance, healthy politics, expression, and economic opportunities in the country of origin as they enjoy the same in the settled countries (Kurtenbach 2017). I posit that spatial transnationalism hinges on the collective consciousness of heterogeneous people who are detribalised and de-ethnicised but bonded by the anticipation of correcting the sociopolitical ills outside the geographical boundary of their country of residence. Spatial transnationalism, therefore, helps generate collective identity, which, according to Taylor and Whittier (1992), involves three main components – collective identity boundaries, consciousness, and the politicisation of everyday life.

In this context, with the proliferation and accessibility of digital media, these transnational actors are closer to home and more prone to criticise and hold accountable the government of the country of origin. In the case of Nigeria, the political involvement of the diaspora allows criticism not only of the Nigerian government and the system in place at home but also of foreign governments considering assistance to the unforthcoming system. For instance, the period before and during the 2023 general elections was characterised by the active political participation of the diaspora. While media sensationalism projected

anti-government (APC) conversations and promoted the populist mantra of Peter Obi, there were numerous X–Twitter spaces hosted by @PeterObiUSA, a group of Nigerians in the diaspora who are canvassing votes for Peter Obi – the Labour Party's presidential candidate. These spaces gathered huge followers, promoted Obi as a premium candidate, and served as grounds for (dis) information and (mis)information (Garba 2023). Among the diaspora were those who did not support Obi's candidacy, although critical of the Buhari-led APC government, but still preferred Bola Tinubu as the next president, even though he is part of the APC. Following the elections, while the winning APC party celebrated their victory and received congratulations from the US State Department, which considered the elections as a "competitive election" . . . "representing a new period for Nigerian politics and democracy," among the Nigerian diaspora and others concerned about the election's outcome, there was rather a venting of anger toward the US government (Gramer 2023).

Conclusion

The dynamic phenomenon of the internet and the proliferation of social media platforms bear testimony to the role of technology in driving social change. Today, our social world is experiencing profound transformations brought about by digital technologies, expanding the scope of visibility politics and consequently heightening the precarious nature of identity politics. While this chapter's focus revolves around the politics of Nigeria before and after its recent general elections, the depicted scenario is not far removed from what is observed elsewhere globally. Coupled with sociopolitical and economic grievances, the widespread use of social media has significantly facilitated digital populists in exploiting existing fault lines and grievances, positioning themselves as emergent leaders who capitalise on prevailing sentiments. Digital populism has fueled increased ethno-tribal and political polarisation, not confined to Nigeria but evident across various parts of the world. This phenomenon is also notable in the context of spatial transnationalism, prevalent in many countries in the era of digital media technologies. While spatial transnationalism has been a persistent feature in countries like Iran and India, its prominence was particularly evident during the recent controversial elections in Pakistan. Rather than simply attributing (mis)information and (dis)information solely to digital media platforms, a complex approach is to equally acknowledge the role they play in facilitating new modes of thinking, challenging established regimes of truths, and questioning hierarchies of truth. This approach raises several pertinent questions, including but not limited to the authenticity of political narratives, contestation of political space, legitimacy of democratic processes, social cohesion, and the dynamics of identity and generational politics. It serves as a wake-up call for established

regimes, indicating that politics cannot remain static; there will always be contestation of narratives aimed not at overthrowing existing structures and establishments but rather at improving the state and its politics.

Notes

1 https://twitter.com/thecableng/status/1620050223937769472?lang=en https://twitter.com/CDDWestAfrica/status/1618606192301084672?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1618606192301084672%7Ctwgr%5E73f18e478d72786d7d8bfc44c5c8218dcaa81bac%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.aljazeera.com%2Ffeatures%2F2023%2F2%2F15%2Fnigeria-election-triggers-deluge-of-fake-news-on-social-media

2 https://twitter.com/PeterObi/status/1679380422063521792

References

Akinkuotu, Eniola. 2022. "Nigeria 2023: Can Support from Mega Churches Boost Peter Obi's Chances?" *The Africa Report*, December 1. https://www.theafricareport.com/264709/nigeria-2023-can-support-from-mega-churches-boost-peter-obis-chances/

Alabi, Tope. 2023. "May 29: Tweeps Criticise Incoming Administration, Trend." #TinubuIsnotMyPresident. *Punch*, May 28. https://punchng.com/may-29-tweeps-criticise-incoming-administration-trend-tinubuisnotmypresident/

Allison, Graham T., Conrad Black, Eric Edelman, Zalmay Khalilzad, Robert Legvold, Michael Lind and Robert W. Merry. 2017. "America and Russia: Permanent Confrontation?" *The National Interest* (151): 5–24.

Arif, Hajira and Najimdeen Bakare. 2022. "Health Security, Vaccine Hesitancy and Post-truth: A Case of COVID-19 in Pakistan." *Journal of Asian and African Studies* 59 (4): 1135–1153. https://doi.org/10.1177/00219096221130344

Bakare, Najimdeen. 2021. "Edward Azar's Protracted Social Conflict Theory and Drivers of Self Determination: The Case of Nigeria." *Przeglad Strategiczny* (14): 313–327.

Bakare, Najimdeen. 2024. "Self-Determination and Secessionism in Nigeria: A Contextual Analysis through Edward Azar's Protracted Social Conflict Theory." *Journal of Contemporary African Studies* 42 (4): 564–580. https://doi.org/10.1080/02589001.2024.2390384

Ball, Jame. 2017. *Post-truth: How Bullshit Conquered the World*. London: Biteback Publishing.

Berger, John. 1972. *Ways of Seeing*. New York: Penguin.

Bernstein, Mary. 2005. "Identity Politics." *Annual Review of Sociology* 47–74.

Brighenti, Andrea. 2007. "Visibility: A Category for the Social Sciences." *Current Sociology* 55 (3): 323–342. https://doi.org/10.1177/0011392107076079

Brighenti, Andrea. 2010. *Visibility in Social Theory and Social Research*. New York: Springer.

Bucher, Taina. 2012. Want to Be on the Top? Algorithmic Power and the Threat of Invisibility on Facebook. *New Media & Society* 14 (7): 1164–1180. https://doi.org/10.1177/1461444812440159

Busari, Biodun. 2022. "2023: Peter Obi Represents Body, Soul of Igbo – Ohanaeze." *Vanguard*, November 23. https://www.vanguardngr.com/2022/11/2023-peter-obi-represents-body-soul-of-igbo-ohanaeze/#google_vignette

The Cable. 2023. "Is Peter Obi a Religious Bigot as His Critics Claim?" *The Cable*, April 6. https://www.thecable.ng/is-peter-obi-a-religious-bigot-as-his-critics-claim

Casper, Jayson. 2023. "Nigerian Christians Explain High Stakes of 2023 Presidential Election." *Christian Today*, February 24. https://www.christianitytoday.com/news/2023/february/nigeria-election-2023-christians-peter-obi-tinubu-abubakar.html

Creech, Brian. 2020. "Exploring The Politics of Visibility: Technology, Digital Representation, and the Mediated Workings of Power." *Semiotica* 2020 (236–237): 123–139. https://doi.org/10.1515/sem-2018-0043

D'Ancona, Matthew. 2017. *Post-truth: The New War on Truth and How to Fight Back*. New York Random House.

Davis, Evan. 2017. *Post-truth: Why We Have Reached Peak Bullshit and What We Can Do About It*. New York: Little Brown.

De Backer, Mattias. 2019. "Regimes of Visibility: Hanging out in Brussels' Public Spaces." *Space and Culture* 22 (3): 308–320. https://doi.org/10.1177/1206331218773292

Farkas, Jannick and Johan Schou. 2020. *Post-Truth, Fake News and Democracy: Mapping The Politics of Falsehood*. New York: Routledge.

Federal Ministry of Youth and Sports Development in Collaboration with National Bureau of Statistics. 2020. "National Youth Survey 2020." https://nigerianstat.gov.ng/elibrary/read/1241079

Foroughi, Hamid, Gabriel, Yiannis and Marianna Fotaki. 2019. "Leadership in a Post-Truth Era: A New Narrative Disorder?." *Leadership* 15 (2): 135–151. https://doi.org/10.1177/1742715019835369

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. London: Penguin.

Foucault, Michel. 1979. *The History of Sexuality: Volume 1*, Robert Hurley (trans.). New York: Vintage.

Garba, Mahdi. 2023. "Twitter Spaces 'Spreading Disinformation in 2023 Elections." *HumAngle*, March 10. https://humanglemedia.com/twitter-spaces-spreading-disinformation-in-2023-elections/

Ghosh, Biswajit. 2022. "Politics of Manufacturing Consent in a Post-Truth Society." *Journal of Developing Societies* 38 (1): 7–26.

Gordon, Neve. 2002. "On Visibility and Power: An Arendtian Corrective of Foucault." *Human Studies* 25: 125–145.

Gramer, Robbie. 2023. "Election Results While Election Observers Cried Foul." *Foreign Policy*, March 6. https://foreignpolicy.com/2023/03/06/nigeria-elections-us-biden-democracy-africa-tinubu/

Guardian. 2021. "The Growth of Smartphone Usage in Nigeria." *Guardian*, April 1. https://guardian.ng/technology/the-growth-of-smartphone-usage-in-nigeria/

Harding Luke, Julian Borger and Dan Sabbagh. 2021. "Kremlin Papers Appear to Show Putin's Plot to Put Trump in White House." *The Guardian*, July 15. https://www.theguardian.com/world/2021/jul/15/kremlin-papers-appear-to-show-putins-plot-to-put-trump-in-white-house

Hazzan, Kayode Mosses. 2023. "Deception in the Era of Digital Technologies and the Distortion of Reality and Facts: An X-Ray of Nigerian Peculiarities." *E-Learning and Digital Media* 20(6), 563–578. https://doi.org/10.1177/20427530221124002

Jiménez-Martínez, Cesar. 2021. "The Instrumental Mediated Visibility of Violence: The 2013 Protests in Brazil and the Limitations of the Protest Paradigm." *The International Journal of Press/Politics* 26 (3): 525–546. https://doi.org/10.1177/1940161220923984

Jiménez-Martínez, Cesar and Lee Edwards. 2023. "The Promotional Regime of Visibility: Ambivalence and Contradiction in Strategies of Dominance and Resistance." *Communication and the Public* 8 (1): 14–28. https://doi.org/10.1177/20570473221146661

Klandermans, P. G. 2014. "Identity Politics and Politicized Identities: Identity Processes and the Dynamics of Protest." *Political Psychology* 35: 1–22.

Kurtenbach, Sebastian. 2017. "Spatial Transnationalism: An Analytical Approach." In *The New Diversity of Family Life in Europe*, edited by Banu Çitlak, Sebastian Kurtenbach, Megan Lueneburg and Meglena Zlatkova. Wiesbaden: Springer.

Luckscheiter, Jochen. 2022. "Bots and Biases: The Role of Social Media in Nigeria's Elections." *Heinrich Boll Stiftung*, October 26. https://ng.boell.org/en/2022/10/26/bots-and-biases-role-social-media-nigerias-elections

Mayer, Jane. 2018. "How Russia Helped Swing the Election for Trump." *The New Yorker*, September 24. https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump

Mureithi, Carlos. 2023. "Can Nigerian 'New Broom' Candidate Sweep the Youth Vote?." *Christian Science Monitor*, February 24. https://www.csmonitor.com/World/Africa/2023/0224/Can-Nigerian-new-broom-candidate-sweep-the-youth-vote

Ndubuisi, Olivia and Nduka Orjinmo. 2023. "Nigeria Election 2023: Who is Peter Obi of the Labour Party?." *BBC*, February 23. https://www.bbc.com/news/world-africa-61865502

Neumayer, Christina and Luca Rossi. 2018. "Images of Protest in Social Media: Struggle Over Visibility and Visual Narratives." *New Media and Society* 20 (11): 4293–4310. https://doi.org/10.1177/1461444818770602

Nwonwu, Chiagozie, Fauziyya Tukur and Olaronke Alo. 2023. "Nigeria Elections: Websites Use False Stories to Attract Views and Ads." *BBC*, September 14. https://www.bbc.com/news/world-africa-66647768

Obadare, Ebenezer. 2023. "What Now for the Igbo?" *Council on Foreign Relations*, March 13. https://www.cfr.org/blog/what-now-igbo

Olabanjo, Olusola, Ashiribo Wusu, Oseni Afisi, Mauton Asokere, Rebecca Padonu, Olufemi Olabanjo, Oluwafolake Ojo, Olusegun Folorunso, Benjamin Aribisala and Manuel Mazzara. 2023. "From Twitter to Aso-Rock: A Sentiment Analysis Framework for Understanding Nigeria 2023 Presidential Election." *Heliyon* 9 (5): 1–14.

Opejobi, Seun. 2023. "PEPT Judgement: Peter Obi has Made Christians Unable to Condemn Muslim Presidential Candidates – Omokri." *Dailypost*, September 7. https://dailypost.ng/2023/09/07/pept-judegment-peter-obi-has-made-christians-unable-to-condemn-muslim-presidential-candidates-omokri/

Phillips, Samuel. 2022. "The Peter Obi Movement: Political or Spiritual?" *Msingi Afrika Magazine*, July 11. https://www.msingiafrikamagazine.com/2022/07/the-peter-obi-movement-political-or-spiritual/

Rega, Isabella and Andrea Medrado. 2023. "The Stepping into Visibility Model: Reflecting on Consequences of Social Media Visibility – a Global South Perspective." *Information, Communication & Society* 26 (2): 405–424.

Salako, Pelumi. 2023. "Nigeria Election Triggers Deluge of 'Fake News' on Social Media." *Aljazeera,* February 15. https://www.aljazeera.com/features/2023/2/15/nigeria-election-triggers-deluge-of-fake-news-on-social-media

Schiller, Glick Nina, Linda Basch and Cristina Blanc-Szanton. 1992. *Transnationalism: A New Analytic Framework for Understanding Migration: A New Analytic Framework*. New York: Willey.

Taylor, Verta and Nancy Whittier. 1992. "Collective Identity in Social Movement Communities: Lesbian Feminist Mobilization." In *Frontiers in Social Movement Theory*, edited by Aldon D. Morris and Carol M. Mueller, 104–129. New Haven: Yale University Press.

Thorburn, Elise. 2014. "Social Media, Subjectivity, and Surveillance: Moving on from Occupy, The Rise of Live-streaming Video." *Communication and Critical/Cultural Studies* 11(1): 52–63. https://doi.org/10.1080/14791420.2013.827356

Uldam, Julie. 2018. "Social Media Visibility: Challenges to Activism." *Media, Culture and Society* 40 (1), 41–58. https://doi.org/10.1177/0163443717704997

Van Stekelenburg, Jacquelien. 2013. "Collective Identity." In *The Wiley-Blackwell Encyclopaedia of Social and Political Movements*, edited by David Snow, Donnatella Della Porta, Bert Klandermans and Doug McAdam, 219–225. Malden, MA: Wiley-Blackwell.

Whittier, Nancy. 2009. "The Visibility Politics: Coming Out, Activist Art, and Emotional Change." In *Politics of Child Sexual Abuse: Emotion, Social Movements, and the State*, 167–181. Oxford: Oxford University Press.

Whittier, Nancy. 2018. "Identity Politics, Consciousness Raising, and Visibility Politics." In *The Oxford Handbook of U.S. Women's Social Movement Activism*. https://nancywhittier.files.wordpress.com/2018/02/identity-politics-consciousness-raising-and-visibility-politics-oxford-handbook-postprint.pdf

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

PART 2

Conspiracy Theories

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

4

THE PERSISTENCE OF INFORMATIONAL MANIPULATION AND THE APPROPRIATION OF EMERGING EVENTS

Conspiratorial Publics

Katherine M. FitzGerald, Daniel Whelan-Shamy, and Timothy Graham

Introduction

As the global political climate has shifted toward various forms of right-wing, populist politics that seek to establish dominance over accepted history and facts (Wike et al., 2024), many conspiracy theories have become integrated into mainstream political discussion. Conspiratorial discourse – for example, the idea that the 2023 Maui wildfires were a targeted government operation – within both domestic and international politics has become consistently present in debate on popular social media platforms.

Concurrent to the proliferation of increasingly visible conspiratorial discourse, there has been a surge in scholarly interest in conspiracy theories in recent years (e.g., Douglas et al., 2019; Mahl et al., 2022). However, despite these efforts we are yet to develop an understanding of how groups of conspiracy theorists iteratively add new events into an existing repository of beliefs. While this is a core strategy that conspiracy theory communities employ to theorise how power operates and to provide empirical "evidence" for the narratives supporting these theories, we are not aware of any studies that focus on how these groups appropriate new events – such as natural disasters and public health crises.

Scholars grappling with conspiracy theories are often left wondering what elements of a conspiratorial narrative enable it to persist and gain traction across a wide user base. We address this gap in knowledge by providing an account of the nature of networked communication, specifically the tactics that groups of conspiracy theorists use to develop narratives over time. We specifically concentrate on the role of digital architecture and affordances of these platforms in facilitating the formation of communities that leverage

DOI: 10.4324/9781003628088-6
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

the technical and social nature of digital platforms to develop, maintain, and spread a high volume of conspiracy theories while also including new events into their narrative system.

We call communities who leverage the role of digital affordances to maintain conspiratorial narratives, "conspiratorial publics." In this chapter, we explain how conspiratorial publics fit within the framework of SDIOs discussed in this volume and work to differentiate conspiratorial publics from other theories of publics. As we define them, conspiratorial publics are a type of public dedicated to the maintenance and development of conspiracy theories that maintain a consistent presence on digital platforms that never completely disappear. We argue that conspiracy theories persist due to a dynamic interaction between the social nature of digitally mediated communication and the technical affordance of the social platforms where mediated communication takes place. In our framework, a "conspiracy theory" refers to the theory itself – for example, flat earthers or QAnon – but a "conspiratorial public" refers to a broader construction of conspiracy theorists that are not necessarily constricted to one specific conspiracy theory. Instead, a conspiratorial public is typified by its members who share a similar belief system and utilise a methodology that encourages performative criticality toward historical and current events.

To elaborate on the ideas introduced earlier, in this chapter we focus on two interconnected factors that are constitutive of conspiratorial publics and are also central to the conduct of SDIOs as described by Ihsan Yilmaz and Sharam Akbarzadeh in their introductory chapter to this volume. Elsewhere, Yilmaz and Akbarzadeh have written that SDIOs refer to "efforts by state and non-state actors to manipulate public opinion . . . [and] deliberate alteration of the information environment by social and political actors to serve their interests" (Yilmaz et al., 2023). Conspiracy theorists, by equal measure, manipulate technical affordances such as co-hashtagging – a practice that involves pairing "mainstream" hashtags with those linked to conspiratorial content – to amplify the visibility and reach of the conspiratorial narratives within the wider information environment of social media platforms. Conspiracy theorists use conspiratorial narratives as a form of information control that sits at the intersection of political action and the productivity of online fandoms (Andrejevic, 2008).

With the major themes of this chapter established, our argument is structured as follows. First, we outline the current literature on conspiracy theories. We also discuss social media affordances and the role that the technical design of platforms plays in facilitating conspiratorial communication. Thereafter, we turn to discuss publics as part of mediated communication. Following this literature review, we introduce our theoretical contributions to the field – namely, the idea of "conspiratorial publics." We operationalise these ideas using a case study of the spread of conspiratorial discourse as it related

to the 2023 Maui wildfires on X, formerly known as Twitter. We focus our analysis on the user practice of co-hashtagging as it is a definitive part of the overall #MauiPsyOps SDIO and of conspiratorial publics more broadly. We conclude with brief reflections on the implications of this chapter as well as avenues for future work.

Enduring Logic of Conspiracy Theories: Recurring Tropes and Continuing Communities

There is a lack of consensus among scholars regarding the definition of conspiracy theories, particularly as they have moved into the online world. In 2022, Mahl and colleagues conducted a meta-analysis of conspiracy theory literature in response to the increased number of papers in this space to determine if papers included a definition and, if so, what was the most common definition of a conspiracy theory. The study identified the most often used definition to be from Sunstein and Vermeule's work. They proposed that conspiracy theories are "an effort to explain some event of practice by reference to the machinations of powerful people, who attempt to conceal their role" (Sunstein and Vermeule, 2009, 205). While this is the most frequent definition, the common thread of the other most prominent definitions was that two or more actors were involved, and that their malevolent goals were kept secret (Douglas et al., 2019; Mahl et al., 2022; Zonis and Joseph, 1994).

Noteworthy within the literature on conspiracy theories is that the same allegations and tropes appear repeatedly in different theories and across "time, cultures, and social settings" (Prooijen and Douglas, 2018, 897). While some conspiracy theories turn out to be legitimate – for example, some allegations of corporate corruption were in fact conspiracies – many more of these theories are implausible or even impossible if logic and scientific knowledge are applied (Prooijen and Douglas, 2018). The range of possibilities from flat earthers to valid accusations of corruption points to a wide range in the level of plausibility and refutability among conspiracy theories.

Examples of common themes among conspiracy theories include anti-establishmentarianism, cover-ups by officials, and "othering" of minority and religious groups (Enders et al., 2022; Prooijen and Douglas, 2018). Anti-establishmentarianism is an attitude of opposition to an institution's power structure and being "hostile to the social, economic, and political principles of nation's ruling class" (Merriam-Webster Dictionary, 2024). Common in anti-establishment conspiracy theories is the attribution of intentionality and placing of blame on a shadowy group of elite figures; a common trope that connects many conspiracy theories and has persisted across contexts and time (Prooijen and Douglas, 2018; Douglas et al., 2019). Historical examples of blaming shadowy elites include attributing blame for the Great Fire of Rome to Emperor Nero; statements that the assassination of President

John F. Kennedy was orchestrated by the CIA; or that the RMS Titanic was sunk to kill supporters of the newly proposed Federal Reserve (Zelikow and Holland, 2002; Trickey, 2018).

Despite this long history of common themes, there is a lack of scholarship explaining how the same narratives and tropes appear across conspiracy theories related to different events. The idea of wildfires being intentionally caused, rather than believing the official explanation of events, is representative of an enduring trope that is likely to be reiterated across similar natural disasters. Attempts have been made to bridge the gap in the literature relating to conspiracy theory practices and their enduring nature. However, this literature fails to describe the *extensive community of online users and their communal practices, which are persistently present* in online environments; users who stand ready to amplify a wide range of conspiracy theories utilising various affordances that are applicable across platforms.

Important contributions that attempt to understand conspiracy theories from an epistemic or community practice point of view include the theory of populist expertise from Marwick and Partin (2022) and the idea of participatory disinformation put forward by Kate Starbird et al. (2019, 2023). The theory of populist expertise focuses on epistemology and examines collective and knowledge-making practices of QAnon conspiracy theorists which can be applied to other conspiratorial narratives (Marwick and Partin, 2022). Marwick and Partin (2022) proposed populist expertise as a way of understanding the collective and systematic knowledge-making practices that are inherent to QAnon and define it as: "the rejection of legacy media accounts, scientific consensus, or elite knowledge in favour of a body of 'home-grown' forms of expertise and meaning making generated by those who feel disenfranchised from mainstream political participation" (2). Despite the term's contribution to understanding conspiratorial epistemology, populist expertise does not entirely capture the industriousness and collective user practices that are inherent to conspiratorial communities of online users who amplify a wide range of conspiracy theories across platforms and emerging events.

We assert that these communities – or publics – are partial drivers of the recurring nature of conspiratorial tropes. The productive labor that these conspiracy theorists are involved in is not accounted for by the previous literature and does not acknowledge that users are making a concerted effort to keep narratives in the limelight and as consistent elements of an overarching story. By having a consistently present public driving this messaging, it ensures the narrative's survival when conspiracy theories such as #MauiPsyOps might disappear quickly into the ether of the Internet.

Social Media Architecture and Its Role in Conspiracy Theories

Social media users congregate around conspiracy theories – similarly to the way users come together around an issue public – that have no widely

accepted evidence from the scientific community as to their existence. In this sense, there is an epistemic dimension at play in that members employ their own mode of empiricism that generates "evidence" to solicit belief in their claim's assertions, while simultaneously these conspiracy theorists work to refute or discredit outside opinion or evidence (Simion, 2023a, 2023b). This flawed, collectivised mode of knowledge production constructs a different kind of expertise and authority than what we traditionally accept in other domains such as science and is indicative of the methodology that conspiracy theorists use to construct conspiratorial canon as we illustrate it in the following sections.

Rather than characterising disinformation as just another kind of information, Mona Simion (2023a) argues that disinformation is unique in its capacity to generate *false belief* and consistent ignorance. False belief is not just believing in something erroneous; it also comes with the *disposition* to *transmit this false belief and ignorance in future discourse many times over* (Simion, 2023a). In place of conventional experts, the epistemic model that members of conspiratorial publics labor under grants authority to fringe actors who can utilise collective sensemaking and populist expertise to promote narratives that encourage the proliferation of false belief (Simion, 2023a) that are often believed, engaged with, and traded up the chain.

The affordances of social media are critical to conspiratorial publics. Affordances are features of social media platforms that allow for mediation and connection between users and a platform (Bucher and Helmond, 2018). Reposts, quote tweets, likes, and view counts become the "validators" of claims made in posts and comments. These affordances can be leveraged by users to spread their beliefs through reposting and sharing to increase engagement. It is also a design feature of platforms that institutional knowledge from government agencies or emergency services is presented alongside and in the same manner as posts from conspiracy theorists; this gives the visual cue that the information presented is equally valid. For example, trending lists contain genuine *and* conspiratorial hashtags next to each other and do not differentiate the process that led to their algorithmic amplification. This may lead some users to perceive the claims or assertions linked to such hashtags as epistemically sound.

In 2023, Laufer and Nissenbaum expanded on the idea of algorithmic amplification and its connotations for social trust. They focus specifically on *problematic* algorithmic amplification. This is the proliferation of content such as hate speech, misinformation, and conspiracy theories through the ability of platforms to algorithmically amplify the reach of content, whether it be widespread or selectively for individual users (Laufer and Nissenbaum, 2023). Amplification can

> be further intensified due to the dynamic effects of the initiating steps; for example, people whose beliefs, incentives, and behaviours have been

> affected by amplified content may further amplify this content in their interactions with one another or with the platform.
>
> *(Laufer and Nissenbaum, 2023, 6)*

Groups of conspiracy theorists can gain outsized attention because of how platforms algorithmically curate and regulate content. It allows conspiracy theories such as #MauiPsyOps, discussed further in our case study, to gain traction online. It is not purely problematic algorithmic amplification that ensures conspiracy theories continue to receive visibility and shares. This can also be attributed to the work and industriousness of conspiracy theorists in these online communities, who engage in knowledge production to ensure that conspiratorial narratives continue to propagate, while using the affordances of reposts and likes to interact with conspiratorial narratives and further promote them.

Beyond the Moment: How Conspiratorial Publics Persist in Technosocial Networked Environments

Scholars researching the internet in recent years have been interested in understanding the nature of networked communication. Our account of "conspiratorial publics" is built on a lineage of scholarship that is interested in discussing the intersection of "people, technology, and practice" (boyd, 2010, 39). In emphasising the importance of conspiratorial publics, we briefly discuss the literature on publics to articulate the contribution of conspiratorial publics as a theoretical framework for studying the practices and discourse of conspiratorial communities.

Traditionally understood, a public is made up of people to gather to exchange ideas, news, and culture. A public becomes "networked" when technically facilitated architectures of communication that are provided by social media platforms, their algorithms, and technical logics become integral to the conduct of communication (boyd, 2010). As the importance of understanding the nature and dynamics of networked communication has grown, so too has the scholarship focusing on emerging kinds of publics.

For instance, issue publics have become a common analytic framework to understand how groups of communicators who – often prompted by a global development such as a natural disaster or entertainment event – come together to discuss their shared interest for a short period of time (Bruns, 2023). Ryan and Ehlinger build upon Philip Converse's essay on mass belief systems to articulate their view and definition of issue publics (2023). Their definition is similar to that proposed by Bruns but is elaborated to state that one of the key elements of issue publics is an emotional component of interest or excitement. Members will have a long-standing interest in an issue, and care significantly about this issue compared to others (Ryan and Ehlinger,

2023). From a political psychology perspective, an issue public is a "segment of voters with crystallised attitudes about a particular topic" (Ryan and Ehlinger, 2023, 19). Examples of these topics within the political sphere could be gun rights or abortion rights advocates; these are often single-issue politics that are supported by a consistent issue public.

Differing from issue publics is the idea of "ad hoc" publics (Bruns and Burgess, 2015). In ad hoc publics, hashtags are a means of coordinating discussion about specific events, themes, and topics (Bruns and Burgess, 2015). Users of Twitter, and other platforms with the hashtag affordance, can follow and post specific hashtag conversations that formed around emerging events (Bruns and Burgess, 2015). Ad hoc hashtags are used for coordinating discussion and can emerge as a central space to share information about an emergency such as a natural disaster. It is unsurprising, then, that hashtags would emerge around our case study of the 2023 Maui fires; this ad hoc public grew particularly quickly as there was limited phone reception and television coverage following the disaster, which left a vacuum for social media to fill with their own interpretation of the events (Bruns and Burgess, 2015; Kelly, 2023). Ad hoc publics and the spread of misinformation or conspiracy theories are of epistemic relevance when situations are uncertain, such as in an unfolding emergency (Sternisko et al., 2020).

Conspiratorial publics differ from ad hoc publics (Bruns and Burgess, 2015) in that they are consistently present, rather than being formed in response to a crisis or unfolding event. Conspiratorial publics are consistently sustained with hashtag campaigns and collective sensemaking that adds a constant stream of positive "evidence" that affirms conspiratorial tropes and provides space to evolve narratives and theories. While ad hoc publics are ephemeral and will form around discursive events – for example, the #TurkiyeSyriaEarthquake hashtag public in 2023 – conspiratorial publics are enduring.

Another way in which conspiratorial publics differ from existing frameworks is that the latter form around inarguably real events that have been verified – for example, a geopolitical conflict, election, or natural disaster. An example of a long-term issue public would be Black Lives Matter. This issue public differs significantly from conspiratorial publics in that it is a form of activism responding to very real issues of police brutality and discrimination against people of color. In contrast, conspiratorial publics lack legitimacy and form around topics that cannot be proven and are not necessarily real. An example of a conspiratorial public is the online community that utilised the #SaveTheChildren hashtag to push the QAnon conspiracy theory which involved multiple debunked claims.

Conspiratorial publics involve a mode of empiricism that has the *trappings* of scientificity in that "evidence" is collected, and members of the community are encouraged to do their own research. Key dimensions of the scientific method of empiricism are missing from conspiratorial publics: chiefly,

verification, and falsifiability. Members of conspiratorial publics engage in a crude imitation of the scientific method but base their "findings" on flawed epistemologies and community sensemaking practices. Conspiratorial publics qualitatively differ from ad hoc publics in that the latter would exist regardless of the collective work of conspiracy theorists. There are tangible reasons for ad hoc publics to exist – for example, to collate information about an unfolding global development. Conspiratorial publics require maintenance to keep them alive after other traditional forms of media have moved on – they serve to "connect the dots" in between major events and thereby sustain the conspiratorial discourses and social interactions.

Conspiratorial Canon: The Productive Epistemology of Conspiratorial Communities

As we employ it in this chapter, conspiratorial canon works as a guiding narrative function and serves as the "hook" on which a developing event can be caught on and thereby incorporated into an existing conspiratorial narrative. In fiction, canon is defined as "the body of works taking place in a particular fictional world that are widely considered to be official or authoritative; [especially] those created by the original author or developer of the world" (Oxford English Dictionary, 2024). Contemporary fandom is viewed as a highly communal genre, and accordingly we assert that conspiratorial canon positions conspiracy theorists similarly to "fans," and encourages engagement with existing material that then is communicated back and forth among other community members.

Social media platforms have changed the way that people view and interact with breaking news and developing stories. Studying the interactions between reality TV producers and online fans, Andrejevic (2008) has argued that the productivity of online fandoms has resulted in a blurring of the production and consumption divide that has resulted in the critical or hateful reading of a show, its cast, content, and marketing material because it produces value for a franchise. Furthermore, the encouragement of intense criticality comes laden with the expectation that over time, fans will imagine themselves in the role of producer so that they will be able to "imagine the imperatives that shape the programming they consume" to see through the veneer of commercial production that guides the creation of commercial television (Andrejevic, 2008, 39).

We also see this logic at work in conspiratorial publics. An intense criticality of simple coincidence or erroneous reporting that encourages the conspiratorial subject to present themselves as being unable to be duped by the alleged "producers" of the world in which we live (Andrejevic, 2008). It is through this logic that conspiratorial canon becomes a centerpiece of conspiratorial communities as they work to untangle the supposed lies of the powers that

be. Indeed, it is through the maintenance and incorporation of new events into conspiratorial canon that these "fictions" become actualised through a radical form of social constructivism (Zeeuw and Gekker, 2023). Through collective practice that is facilitated through the affordances of social media platforms, we see a "productive" culture emerge that envisages the world as a series of interconnected fictions – and by observing them, the conspiratorial subject performs the critical act of self-optimisation; showing that they see through the veneer and cannot be fooled (Andrejevic, 2008; Zeeuw and Gekker, 2023). Such performativity is central to the conduct of conspiracy theorists, yet to date it is underrepresented in the current literature on conspiracy theories and their communities, and practices.

Conspiratorial Publics: From an Ephemeral Feature of Discourse to an Ever-Present Public

At this point, we find that there is a conceptual need to consider the productive nature of conspiratorial communities, as well as their ever-present nature on social media platforms. We call these communities "conspiratorial publics," and define them as:

> networks of individuals who collectively work to promote and sustain conspiratorial narratives on social media and digital platforms. These networks rely heavily on already existing conspiratorial narratives as well as new events that serve as resources to evidence and evolve their shared beliefs over time. Conspiratorial publics are enduring, digitally networked collectives that actively work to sustain and propagate conspiracy theories by *constantly integrating emerging events* into an evolving conspiratorial canon.

Conspiratorial publics are enduring networks of individuals that exist at a low-level "simmer" across platforms for the purpose of developing, maintaining, and promoting conspiracy theories. Members of conspiratorial publics are characterised by a positivist logic that equates the existence of inconsistencies in the narratives that underpin a developing or historical event as being evidence of a larger conspiracy. Members actively seek to perform criticality and undermine developing narratives around acute events that promote epistemic uncertainty. As we will demonstrate in our case study and undermine institutional trust by leveraging the social and technical affordances of social media.

Modern conspiracy theories, such as the QAnon movement, that owe their development largely to the affordances of networked technologies, have been lacking a definition or description that distinguishes them from other historical conspiracy theories and social movements. The practice of consistently

integrating emerging events into a wider conspiratorial narrative can be seen in hashtag campaigns such as #SaveTheChildren, #clotshot, or #Agenda2030. These terms relate to conspiracy theories around child sex-trafficking, the lack of safety and efficacy of the COVID-19 vaccine, and the sustainable development framework Agenda 2030 being a cover-up to introduce a New World Order, respectively. These keywords and hashtags exist at a consistent low-level simmer on digital platforms, waiting for an event to prompt greater engagement and more "evidence" to add to their conspiratorial canon.

We next operationalise our definition of conspiratorial publics through the use of an analytic case study. It contains the elements of a conspiratorial public and exemplifies the malicious tactics employed commonly in SDIOs to manipulate information and promote epistemic uncertainty.

Methods: Data Collection and Ethical Considerations

To gather our data, we used the Twitter application programming interface (API) to collect posts containing the hashtag #MauiPsyOps between August 14 and 22, 2023. This hashtag was chosen as it related to the Maui fires but was rife with conspiratorial discourse. Upon initial qualitative investigation by the authors, posts containing this hashtag appeared to be promoting existing conspiratorial narratives and event-specific claims, while also trying to co-opt and cultivate hashtag publics discussing the fires. Therefore, #MauiPsyOps was purposively sampled because of the high proportion of conspiratorial content surrounding it.

We undertake qualitative reading of one key account who initiated the hashtag to track the spread of conspiratorial narratives as they were being attached to the Maui fires event. The key originator account only has 10,000 followers and can be classified as having a "nano-sized" audience (Starbird et al., 2023). We have anonymised this relatively small account. They will be referred to as @UserM. "Microinfluencers" or users with an audience above 25,000 (Starbird et al., 2023) are assumed to be aware of their audience and work to maintain it through regular communication (Marwick and boyd, 2011). We have therefore chosen to display the usernames of accounts of this size or greater.

Case Study: How the 2023 Maui Fires Became an Alleged Psychological Operation (#MauiPsyOps)

In early August 2023, small fires were reported across Maui and Hawaii islands, but they were largely contained (Napuunoa, 2023). A long period of drought and windy conditions meant that on August 8, the fires intensified to a deadly level that garnered international media attention (Bogel-Burroughs et al., 2023). The intensification of the fires that went on to devastate the community of Lahaina was reported as being caused by intense winds that

downed power lines (Biesecker et al., 2023; Bogel-Burroughs et al., 2023). As of February 2025, the death toll of the Maui fires is 102, making the event the deadliest US wildfire since 1918.

The Maui fires received international media attention. Throughout the crisis, people used information from both traditional and social media to communicate and make sense of the evolving situation. The process of attaining and disseminating accurate information during an unfolding crisis is a complex epistemic event for two main reasons. The first is that people directly or indirectly involved in these events always, already have their own views about the world and the nature of events in it, and second, it is increasingly common that any inaccuracy – no matter how small – can be used by members of the conspiratorial public to undermine narratives and accounts from traditional media and/or government sources. This was the case after the September 11 terrorist attacks where conspirators used an inaccurate report from the BBC on the timing of Building 7's collapse to accuse the media outlet of having prior knowledge of the events of 9/11 before they unfolded (Sardarizadeh, 2021).

Because of these two reasons, it is inevitable that some crisis communication involves misinformation or inaccuracies that provide fertile ground for critical, performative interrogation by conspiratorial publics that result in the development of conspiracy theories; this is especially dangerous as people attempt to regain control and understand the situation that is unfolding around them (Abalakina-Paap and Stephan, 1999; Whitson and Galinsky, 2008). The epistemic uncertainty and lack of situational control were particularly amplified during the Maui fires due to widespread power and telecommunication outages (Kelly, 2023), leaving the community vulnerable to misinformation. Employing the tactics implicit to the development of conspiratorial canon that we described earlier, conspiracy theorists pointed out "inconsistencies" – such as the "observation" that blue houses were left untouched by the fires – that were initially posted using the hashtag #MauiPsyOps and lead to the wider conspiratorial development of the hashtag. These "observations" were amplified through a process of co-hashtagging (including multiple hashtags in one tweet) whereby users included both #MauiPsyOps alongside more mainstream hashtags such as #MauiFires (that at the time was being utilised by news outlets and law enforcement to provide public service announcements) to amplify the conspiratorial claims that they were making.

Tracking the Spread of Community Practice: The #MauiPsyOps Conspiracy Theory as a Conspiratorial Public

The initial X account that began the use of the #MauiPsyOps hashtag is @UserM, seen later reposting a larger and more influential account's messaging and adding their own commentary.

BOX 4.1 THE POST FROM @USERM SHARED BY @WELLNESS INFLUENCER ABOUT AID REACHING MAUI. IT HAS BEEN ANONYMISED DUE TO THE LOW ACCOUNT SIZE OF @USERM.

User M, August 15, 2023

The government is blocking relief to Maui, but the people are resourceful. Here is how they have been bypassing the cruel restrictions.

#LahainaFire #LahainaFires #LahainaPsyOp #MauiPsyOp #Maui #MauiFire #MauiFires #Hawaii #HawaiiFire #HawaiiFires #DEW #WEF #TheGreatReset

The post includes a screenshot from a video of someone riding a jet ski, seemingly delivering aid to Maui.

This post was viewed 1.2 million times at the time of data collection with almost 5,000 shares, and over 13,000 likes.

On the first day of the hashtag, only small fringe accounts shared @UserM's posts. These were accounts with approximately 1,000 followers or less and kept the hashtag at a persistent simmer but were not overly effective in spreading the #MauiPsyOps narrative to a large audience. More widespread amplification of the conspiratorial hashtag from micro- and meso-influencers began in the second and third days after #MauiPsyOps emerged. An account we refer to as @WellnessInfluencer retweeted one of @UserM's tweet on August 16.

BOX 4.2 THE FIRST TWEET CONTAINING THE #MAUIPSYOPS HASHTAG.

User M, August 15, 2023
Nothing to see here, folks! Nothing at all. Move along now!
#Lahaina #LahainaFire #LahainaFires #LahainaPsyOps #MauiPsyOp #Maui #MauiFire #MauiFires #Hawaii #HawaiiFire #HawaiiFires #DEW #WEF #TheGreatReset #15MinuteCities #agenda21 #WarOnHumanity

This post included a repost of another user's post from a right-wing influencer with over 900,000 followers on X, which read:

Breaking Report: Coincidentally the Maui Police Chief John Pelletier was also the Incident Commander during the Las Vegas mass shooting.

@WellnessInfluencer is the anonymised name of an account with 148,000 followers and is run by a self-described "free speech journalist," who publishes a blog related to holistic health news to their sizable audience. However, they also repost a not insignificant amount of right-wing US political content. On August 16, @UserG retweeted @UserM's content to their audience of 268,000 followers, creating further exposure. Next, on August 16 and 18, @YogaInfluencer (not their real account name) retweeted @UserM's tweets to an even larger audience of 346,000 followers. This process is an example of a propaganda tactic known as "trading up the chain," which describes the popularisation of messages from small accounts or outlets via their republishing by larger, more visible platforms, people, or outlets (Krafft and Donovan, 2020; Marwick and Lewis, 2017). Trading up the chain serves as a legitimising moment for empirical efforts of conspiracy theorists as their theories are shown alongside other, more legitimate sources of information (such as fire departments or government agencies).

As can be seen on Figure 4.1, the amplification of the #MauiPsyOps hashtag occurred in a variety of ways and across multiple platforms. As demonstrated in the first post from @UserM shown in Box 4.1, the #MauiPsyOps hashtag was utilised alongside existing conspiratorial and non-conspiratorial hashtags from the outset. Notably, there was a mix of hashtags, some of which were utilised for more general news like #MauiFires, while others such as #WEF and #DEW are used almost entirely to spread conspiratorial narratives. #WEF refers to the World Economic Forum, a non-governmental organisation whose stated mission is to "[engage] political, business, academic, civil society and other leaders of society to shape global, regional and

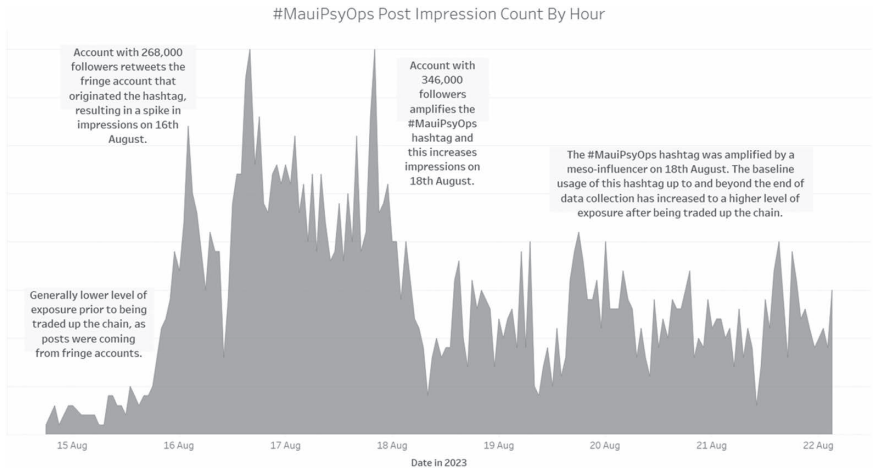


FIGURE 4.1 Visualisation of the volume of the post volume per hour for posts containing #MauiPsyOps.

industry agendas" (World Economic Forum, 2025). The WEF is a popular target for conspiracy theories as members are considered representative of a criminal global elite who do not have the best interests of the population at heart. Directed energy weapons, referred to as #DEW on social media platforms, are referenced in other false narratives surrounding the United Nations' Agenda 2030, the introduction of "smart cities," and climate control. Multiple news outlets noted at the time of the fires that people were falsely claiming the cause was direct energy weapons, and posted refutations and fact checks of these claims (Phan, 2023; Sardarizadeh and Wendling, 2023). Examples such as #WEF and #DEW are indicative of conspiratorial canon, and it is telling that they were included originally alongside the #MauiPsyOps hashtag as these three ideas become associated by proxy.

Through the co-use of central hashtags utilised by ad hoc publics in response to the unfolding crisis, and the hashtags associated with previous conspiracies, @UserM vastly increased the reach of their newly introduced conspiratorial hashtag. By linking the more general #MauiFires with #MauiPsyOps, the latter hashtag could reach a new audience who may engage and spread it even further.

In addition to making observations around co-hashtag usage, as can bee seen on Figure 4.2, we can also break down the spread of the conspiratorial public of #MauiPsyOps into two steps. Initially, we observed a mobilisation period which involved the hashtag originator @UserM and small, fringe accounts reposting their content. During this first stage, we can see the accusatory tone of the conspiratorial public in its fledgling form. The initial tone of the conversation around the Maui fires commented on the disorganisation

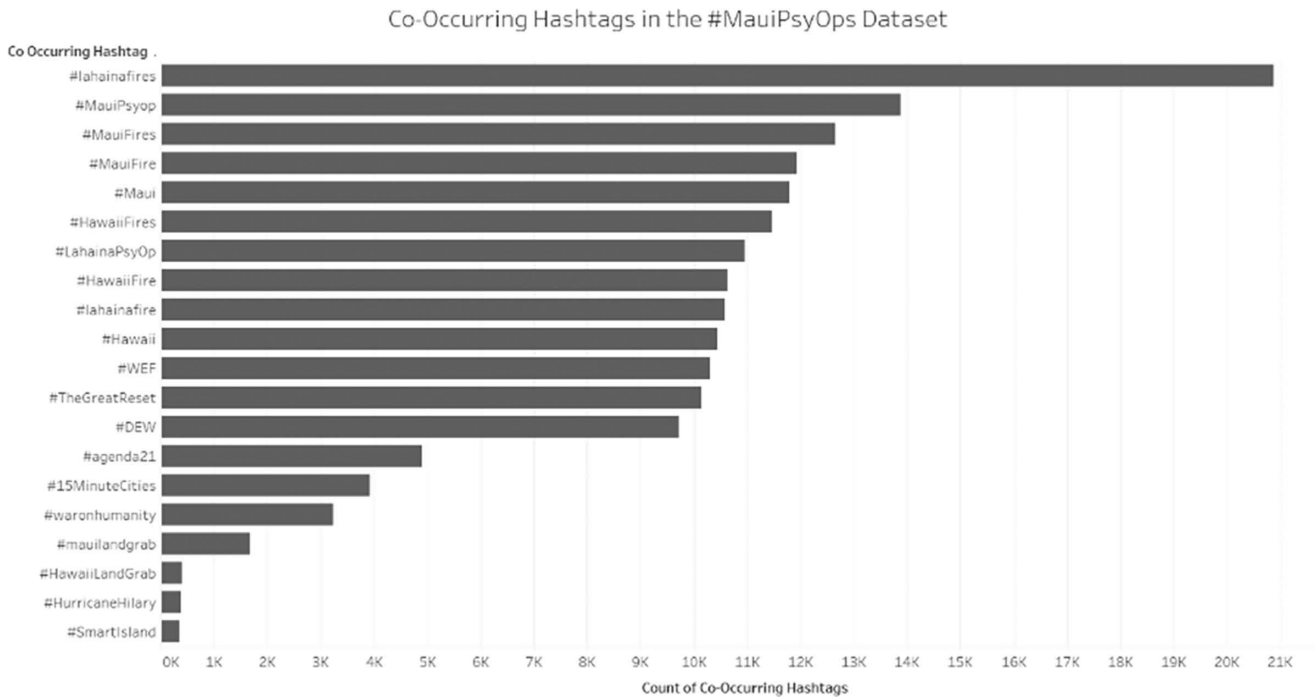


FIGURE 4.2 Visualisation of the hashtags being utilised most frequently in conjunction with #MauiPsyOps.

of the Federal Emergency Management Agency (FEMA) and the delay in delivering aid to the island of Maui. During this period, social media users took advantage of the affordances of the platform to form communities and use multiple hashtags to find one that "stuck" and amplified their messaging. Populist expertise also played a significant role throughout the development of the #MauiPsyOps hashtag as conspiracy theorists are critical of official sources from the government and the institution of FEMA specifically, being distrustful of both the information they are providing and the physical ability for them to respond and assist on the ground during the natural disaster.

As the devastation resulting from the fires became more apparent and an increasing volume of videos and photos of the fire-affected area were made available on social media, users began to ascribe an element of intentionality and blame. This can be seen in Box 4.2, which states: "The government is blocking relief in Maui" and then refers to "cruel restrictions." This second stage of the formation of this conspiratorial public moved from speculation as to why FEMA was delayed, to an active conspiracy that blamed a wide array of groups and individuals from the WEF, the Democratic party, to Oprah Winfrey for the fires. Part of the move toward active conspiracy theorising included the decontextualisation of videos from other social media platforms to share on X, or otherwise misrepresenting information from traditional news outlets. It is at this point that a conspiratorial public became fully formed around #MauiPsyOps as social media users drew on their already existing conspiratorial canon to revitalise narratives seen in previous conspiracies that were then related to the Maui fires.

Co-Hashtagging as an SDIO User Practice

Using co-hashtagging and trading up the chain throughout the course of a developing crisis receiving worldwide attention, @UserM vastly increased the reach of #MauiPsyOps. By linking the more general #MauiFires with #MauiPsyOps, the latter hashtag could reach a new audience who may engage and spread it even further. It is in this way that the #MauiPsyOps hashtag took on a cooperative and seemingly organic form that paired epistemic uncertainty caused by a quickly changing crisis event, with the commercial logics and affordances of social media. These features are indicative of the narrative control and emotional elements that are integral to the conduct of SDIOs (Yilmaz & Akbarzadeh, this volume).

Co-hashtag usage has been seen in previous conspiratorial hashtag campaigns such as #SaveTheChildren, when QAnon co-opted the hashtag campaign of a legitimate charity to spread misinformation and conspiratorial content (Fagan, 2020). We can also see examples of connecting to existing conspiracy theories in @UserM's post containing #DEW. It is evident that unless there is explicit platform intervention to delete this kind of content,

certain hashtags will never entirely disappear from public discourse. For example, hashtags commonly associated with conspiracy theories such as #DEW, #WEF, and #SaveTheChildren appear daily on X, TikTok, and Gab at low but consistent levels. As is characteristic of conspiratorial publics, these hashtags are decentralised across platforms and are consistently reinvigorated by events such as natural disasters and geopolitical tensions, ensuring they never entirely disappear from public view as they continue to be paired with event-based hashtags. Such perennial hashtags are representative of conspiratorial publics as they provide a baseline level of engagement that is easily reinvigorated when paired alongside legitimate hashtags, such as those created in response to a crisis like the Maui fires.

Concluding Notes and Future Directions

In summary, the Maui wildfires are an exemplary case study of a conspiratorial public. We observed the development of a movement from a single account promoting the #MauiPsyOps hashtag to a network of users working to promote and sustain the idea that the Maui fires were lit deliberately for a variety of nefarious reasons. We demonstrated how new events can serve as an opportunity to draw on conspiratorial canon using a malign methodology that is reminiscent of online fandoms (Andrejevic, 2008; Zeeuw and Gekker, 2023).

In doing so, this chapter has introduced the concept of conspiratorial publics to describe how these persistent, networked, and often heterogeneous communities actively sustain and evolve conspiracy narratives over time. By leveraging affordances and the attention economies of digital platforms, these publics co-opt collective sensemaking to integrate emerging events into their broader conspiratorial canon. As a concept, conspiratorial canon explains the recurrence of specific narratives in online conspiracy theories and highlights the industriousness of social media users who actively maintain and propagate these tropes. Furthermore, conspiratorial publics can be understood as a form of SDIO, as their members deliberately manipulate the online information environment to reinforce and disseminate beliefs that align with their ideological interests.

We acknowledge that the case study presented in this chapter is situated within the Anglosphere and is therefore Western-centric. Further work is needed to examine how conspiratorial publics emerge and function outside of Western contexts, particularly in relation to cultural, linguistic, and platform-specific differences that may shape their formation and persistence. While our framework suggests that there are potentially many common features shared across digital environments, future research should explore how localised sociopolitical conditions, digital infrastructures, and algorithmic ecosystems influence the dynamics of conspiratorial publics, as

well as the extent to which these publics intersect with state-sponsored disinformation, grassroots activism, and alternative epistemic norms and practices. Comparative analyses across regions and languages will be particularly valuable in refining the framework and expanding its applicability beyond Western-centric understandings of conspiracy theories.

Index Terms

Key Theoretical Concepts

- Conspiratorial Publics
- Conspiratorial Canon
- SDIOs
- Co-hashtagging
- Trading Up the Chain
- Populist Expertise
- Participatory Disinformation
- Algorithmic Amplification
- Performative Criticality

Conceptual Frameworks Referenced

- Issue Publics
- Ad Hoc Publics
- Fandom Logic
- Digital Affordances
- Epistemic Crisis/False Belief Generation
- Social Constructivism in Online Conspiracy

Conspiratorial Canon Elements

- Directed Energy Weapons (DEWs)
- World Economic Forum (WEF)
- False Flags/PsyOps
- Global Elites/Deep State
- Media Complicity/Prior Knowledge
- Blue Objects Fire Immunity

Platform Affordances Exploited

- Hashtagging
- Retweets and Quote Tweets
- Trending Algorithms

- Visual Interface Equivalence
- Feed Amplification

Phases of Public Formation

1. Mobilisation Phase
2. Amplification Phase
3. Canon Integration
4. SDIO Realisation

References

Abalakina-Paap, Marina, Walter G. Stephan, Traci Craig, and W. Larry Gregory. 1999. 'Beliefs in Conspiracies'. *Political Psychology* 20 (3): 637–647. https://doi.org/10.1111/0162-895X.00160.

Andrejevic, Mark. 2008. 'Watching Television without Pity: The Productivity of Online Fans'. *Television & New Media* 9 (1): 24–46. https://doi.org/10.1177/1527476407307241.

Biesecker, Michael, Bernard Condon, and Jennifer McDermott. 2023. 'Videos Put Scrutiny on Downed Power Lines as Possible Cause of Deadly Maui Wildfires'. *AP News*, 15 August. https://apnews.com/article/hawaii-wildfires-maui-electricity-power-utilities-c46a106db3c5019ac835ddcb01fde25f.

Bogel-Burroughs, Nicholas, Serge F. Kovaleski, Shawn Hubler, and Riley Mellen. 2023. 'Hawaii Wildfires Timeline: How Lahaina Became a Death Trap'. *The New York Times*, 17 August. https://www.nytimes.com/2023/08/15/us/hawaii-maui-lahaina-fire.html.

Boyd, Danah. 2010. 'Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications'. In *A Networked Self*. Edited by Zizi Papacharissi. Routledge.

Bruns, Axel. 2023. 'From "the" Public Sphere to a Network of Publics: Towards an Empirically Founded Model of Contemporary Public Communication Spaces'. *Communication Theory* 33 (2–3): 70–81. https://doi.org/10.1093/ct/qtad007.

Bruns, Axel, and Jean Burgess. 2015. 'The Use of Twitter Hashtags in the Formation of Ad Hoc Publics'. In *Hashtag Publics: The Power and Politics of Discursive Networks*. Edited by Nathan Rambukkana. Peter Lang Publishing Group.

Bucher, Taina, and Anne Helmond. 'The Affordances of Social Media Platforms.' In *The SAGE Handbook of Social Media*. Edited by Jean Burgess, Alice Marwick, and Thomas Poell. SAGE Publications.

Douglas, Karen M., Joseph E. Uscinski, Robbie M. Sutton, Aleksandra Cichocka, Turkay Nefes, Chee Siang Ang, and Farzin Deravi. 2019. 'Understanding Conspiracy Theories'. *Political Psychology* 40 (S1): 3–35. https://doi.org/10.1111/pops.12568.

Enders, Adam, Casey Klofstad, Justin Stoler, and Joseph E. Uscinski. 2022. How Anti-Social Personality Traits and Anti-Establishment Views Promote Beliefs in Election Fraud, QAnon and COVID-19 Conspiracy Theories and Misinformation. *American Politics Research* 51 (2): 247–259. https://doi.org/10.1177/1532673X221139434.

Fagan, Kaylee. 2020. '#SaveTheChildren: How a Fringe Conspiracy Theory Fueled a Massive Child Abuse Panic'. *Media Manipulation Casebook*, 23 March. https://mediamanipulation.org/case-studies/savethechildren-how-fringe-conspiracy-theory-fueled-massive-child-abuse-panic.

Kelly, Samantha Murphy. 2023. 'Why Cell Phone Service Is Down in Maui – and When It Could Be Restored'. *CNN*, 9 August. https://www.cnn.com/2023/08/09/tech/cell-service-outages-maui-fires/index.html.

Krafft, P. M., and Joan Donovan. 2020. 'Disinformation by Design: The Use of Evidence Collages and Platform Filtering in a Media Manipulation Campaign'. *Political Communication* 37 (2): 194–214. https://doi.org/10.1080/10584609.2019.1686094.

Laufer, Benjamin, and Helen Nissenbaum. 2023. 'Algorithmic Displacement of Social Trust'. Knight First Amendment Institute at Columbia University. http://knightcolumbia.org/content/algorithmic-displacement-of-social-trust.

Mahl, Daniela, Mike S. Schäfer, and Jing Zeng. 2022. 'Conspiracy Theories in Online Environments: An Interdisciplinary Literature Review and Agenda for Future Research'. *New Media & Society*, February, 14614448221075759. https://doi.org/10.1177/14614448221075759.

Marwick, Alice E., and danah boyd. 2011. 'I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience'. *New Media & Society* 13 (1): 114–133. https://doi.org/10.1177/1461444810365313.

Marwick, Alice E., and Rebecca Lewis. 2017. *Media Manipulation and Disinformation Online*. New York, NY: Data & Society.

Marwick, Alice E., and William Partin. 2022. 'Constructing Alternative Facts: Populist Expertise and the QAnon Conspiracy'. *New Media & Society*, May, 14614448221090201. https://doi.org/10.1177/14614448221090201.

Merriam-Webster Dictionary. 2024. 'Definition of ANTIESTABLISHMENT'. Accessed 27 February 2024. https://www.merriam-webster.com/dictionary/antiestablishment.

Napuunoa, Nicole. 2023. 'Flights Landing at Maui's Airport While MFD Fights Nearby Fire'. *KHON2*, 4 August. https://www.khon2.com/maui-news/kahului-flights-diverted-due-to-brush-fire/.

Oxford English Dictionary. 2024. s.v. 'canon (*n.1* & *adj.*)'. *Oxford English Dictionary*, September. https://doi.org/10.1093/OED/8893623977.

Phan, Karena. 2023. 'Old Photos Are Being Misrepresented Online to Fuel a Conspiracy Theory about the Maui Wildfires'. *AP News*, 12 August. https://apnews.com/article/fact-check-maui-fire-photos-misrepresented-conspiracy–555091357957.

Prooijen, Jan-Willem van, and Karen M. Douglas. 2018. 'Belief in Conspiracy Theories: Basic Principles of an Emerging Research Domain'. *European Journal of Social Psychology* 48 (7): 897–908. https://doi.org/10.1002/ejsp.2530.

Ryan, Timothy J., and J. Andrew Ehlinger. 2023. 'Issue Publics: How Electoral Constituencies Hide in Plain Sight'. *Elements in Political Psychology*, April. https://doi.org/10.1017/9781009242400.

Sardarizadeh, Shayan. 2021. 'Twitter Suspends 70,000 Accounts Linked to QAnon'. *BBC News*, 12 January, sec. Technology. https://www.bbc.com/news/technology–55638558.

Sardarizadeh, Shayan, and Mike Wendling. 2023. 'Hawaii Wildfires: "Directed Energy Weapon" and Other False Claims Go Viral'. *BBC News*, 14 August, sec. US & Canada. https://www.bbc.com/news/world-us-canada–66457091.

Simion, Mona. 2023a. 'Knowledge and Disinformation'. *Episteme*, June 1–12. https://doi.org/10.1017/epi.2023.25.

Simion, Mona. 2023b. 'Resistance to Evidence and the Duty to Believe'. *Philosophy and Phenomenological Research*, 1–14. https://doi.org/10.1111/phpr.12964.

Starbird, Kate, Ahmer Arif, and Tom Wilson. 2019. 'Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations'. *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–26. https://doi.org/10.1145/3359229.

Starbird, Kate, Renée DiResta, and Matt DeButts. 2023. 'Influence and Improvisation: Participatory Disinformation during the 2020 US Election'. *Social Media + Society* 9 (2): 20563051231177943. https://doi.org/10.1177/20563051231177943.

Sternisko, Anni, Aleksandra Cichocka, and Jay J. Van Bavel. 2020. 'The Dark Side of Social Movements: Social Identity, Non-Conformity, and the Lure of Conspiracy Theories'. *Current Opinion in Psychology* 35 (October): 1–6. https://doi.org/10.1016/j.copsyc.2020.02.007.

Sunstein, Cass R., and Adrian Vermeule. 2009. 'Conspiracy Theories: Causes and Cures*'. *Journal of Political Philosophy* 17 (2): 202–227. https://doi.org/10.1111/j.1467-9760.2008.00325.x.

Trickey, Erick. 2018. 'Fact-Checking QAnon Conspiracy Theories: Did J.P. Morgan Sink the Titanic?'. *The Washington Post*, 4 August. https://www.washingtonpost.com/news/retropolis/wp/2018/08/04/how-j-p-morgan-didnt-sink-the-titanic-and-other-qanon-conspiracy-theories-debunked/.

Whitson, Jennifer A., and Adam D. Galinsky. 2008. 'Lacking Control Increases Illusory Pattern Perception'. *Science* 322 (5898): 115–117. https://doi.org/10.1126/science.1159845.

Wike, Richard, Moria Fagan, and Laura Clancy. 2024. 'Global Elections in 2024: What We Learned in a Year of Political Disruption'. *Pew Research Centre*. https://www.pewresearch.org/global/2024/12/11/global-elections-in-2024-what-we-learned-in-a-year-of-political-disruption/#polarized-battles-over-tradition-and-change

World Economic Forum. 2025. 'Our Mission'. About Us. https://www.weforum.org/about/world-economic-forum/

Yilmaz, Ihsan, and Shahram Akbarzadeh. 2025. 'Introduction: Goals, Practices and Impacts of Strategic Digital Information Operations (SDIOs). In *Authoritarian Actors and Strategic Digital Information Operations: The New Age of Manipulation*. Edited by Ihsan Yilmaz, and Shahram Akbarzadeh. Routledge.

Yilmaz, Ihsan, Shahram Akbarzadeh, and Galib Bashirov. 2023. 'Comprehending the Tactics of Strategic Digital Information Operations (SDIOs)'. 24. Populism and Politics. European Center for Populism Studies (ECPS). https://www.populismstudies.org/wp-content/uploads/2023/09/DOWNLOAD-PDF.pdf.

Zeeuw, Daniël de, and Alex Gekker. 2023. "A God-Tier LARP? QAnon as Conspiracy Fictioning." *Social Media + Society* 9 (1): 20563051231157300. https://doi.org/10.1177/20563051231157300.

Zelikow, Philip, and Max Holland. 2002. 'The Lie That Linked CIA to the Kennedy Assassination'. *Foreign Affairs* 81 (2): 184. https://doi.org/10.2307/20033112.

Zonis, Marvin, and Craig M. Joseph. 1994. 'Conspiracy Thinking in the Middle East'. *Political Psychology* 15 (3): 443–459. https://doi.org/10.2307/3791566.

5

THE ROLE OF SOCIAL MEDIA IN THE DIFFUSION OF CONSPIRACY THEORIES AND THE CONSOLIDATION OF DIGITAL AUTHORITARIANISM IN THE MIDDLE EAST

The Case of Egypt

Ihsan Yilmaz, Ali Mamouri, and Shahram Akbarzadeh

Introduction

In Egypt's 2023 presidential election, the candidacy of independent MP Ahmed al-Tantawi was widely seen as unrealistic in the country's increasingly authoritarian terrain under President Abdel Fattah al-Sisi. Shortly after his announcement, the Egyptian government hacked his phone using Predator spyware, developed by the Israeli company Cytrox (Marczak et al. 2023). Despite this fact, the state-affiliated media launched a smear campaign against al-Tantawi, portraying him as a traitor, an American Israeli spy, and a secret Muslim Brotherhood operative. One conspiracy theory, which has become popular on the Internet, claimed that al-Tantawi is "the Egyptian Zelensky," the Ukrainian president who has risen to global prominence after the Russian invasion of Ukraine in 2022 claimed that al-Tantawi's candidacy is part of a sinister Western conspiracy to get rid of the patriotic army in power and replace its representative al-Sisi with a pro-Western al-Tantawi which will inevitably turn the country into a war zone akin to Ukraine.

Using data from YouTube and Facebook and ten semi-structured interviews with relevant stakeholders, we examine three major conspiracy narratives that have become prevalent in Egypt since the coup in 2013. By doing so, we move beyond the literature's predominant focus on Western countries and English-language communication (Mahl et al. 2023) to examine conspiracy theories in Egypt from Arabic-language sources that emerged since the Russian invasion of Ukraine. This allows for "detecting the nuances in national, cultural, and socio-political differences in the characteristics and impacts of conspiracy theories" (Mahl et al. 2023, 1798).

DOI: 10.4324/9781003628088-7
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

Our investigation shows that three prominent conspiracy theories have gained widespread circulation in Egypt after the Russian intervention in Ukraine. The first theory posits a correlation between Egypt's withdrawal from the International Grains Agreement in 2023, a Western attempt to starve Egypt, and an intelligence collaboration between Russia and Egypt aimed at thwarting the Western scheme against Egypt. The second theory revolves around an alleged Western plot leveraging the economic crisis ensuing from the Ukraine war to instigate chaos within Egypt. The third theory intertwines with the 2023 presidential elections in Egypt, asserting that Western powers are backing civil candidates in opposition to the incumbent President Abdel Fattah Al-Sisi. The alleged objective is to foment a situation akin to Ukraine within the region by replacing Al-Sisi with an "Egyptian Zelensky." Notably, all three conspiracy theories share a triangular construct, wherein the Egyptian leadership is depicted as an autonomous and robust entity, Russia as a steadfast ally, and Western powers as clandestine actors in a conspiratorial framework.

This chapter starts with a discussion of conspiracy theory scholarship, explaining how these conspiracy theories are part of a larger political and historical context. Then, we examine the affordances of social media for disseminating conspiracy theories in Egypt. The next section focuses on three prominent conspiracy theories in Egypt, analyzing their origins, development, and key elements. We discuss the common themes that portray the Western countries and institutions as enemy conspirators against Egypt in contrast to Russia and China as friendly nations.

Conspiracy Theories in the Authoritarian Context

While not necessarily a modern invention, conspiracy theories have become the staple of everyday life in the era of internet technologies and social media communication (Byford 2011). While early research found a negative impact of the Internet on conspiracy theories (Clarke 2007), this trend has been reversed today. In general, the literature has found that social media offers a fertile ground for the proliferation of conspiracy theories on a much larger scale (Cinelli et al. 2022; Douglas et al. 2019).

While it has been widely studied in a Western context, the literature has generally overlooked this phenomenon in the global south and in the Middle East in particular. This study is among a few that focused on this area and Egypt in particular. Second, we contribute to the literature by explaining how a distant geopolitical event (in this case, the war in Ukraine) can be implicated in conspiracy theories. In the context of the Middle East, Gray (2010a) argued that conspiracism is connected to political culture and dynamics in the region. Moreover, and in contrast to Western contexts, conspiracism has been a tool of state communication with society and an explanatory

discourse at the elite as well as more popular street levels. Importantly, the prevalent conspiracy theories can be considered popular interpretations of political dynamics. Gray mentioned a decade ago that what sets the Middle East apart from many other regions is that conspiracism is often part of the state's ideological discourse and not just a discourse by marginalised and dissatisfied minorities. Through conspiracy theories, the state aims to (1) divert attention away from its political and developmental flaws as conspiracism works as a form of state-led Othering and a way of creating a larger imagined enemy; (2) pretend that nothing is changing (during political/economic transition) when in fact it is changing, allowing the state to maintain the rhetoric of earlier ideologies; and (3) create counter-facts that protect the state through misinformation. These state-run conspiracy theories strengthen popular nationalism, divert opposition energies away from the state, and reinforce the state as a source of protection against a perceived enemy. The state disorientates people and reduces their capacity for independent thinking and action (Gray 2010a, 2010b; Koehler-Derrick et al. 2017; Zonis and Joseph 1994).

Another interesting aspect of the Middle East – which is considered the third contribution of this study as well – is that since there have been considerable cases of foreign intervention and actual cases of political conspiracies, such historic precedent gives social and political actors ample cause to be suspicious of conspiracies and plots (Gray 2010b). Our contribution shows how the intertwining of current conspiracy theories in Egypt with the Russian invasion of Ukraine has been influenced by the narratives around the history of foreign conspiracies in the region. Egypt's historical experiences, including periods of colonialism, military interventions, and geopolitical rivalries, provide fertile ground for the proliferation of conspiracy theories that portray external actors as malevolent forces seeking to undermine the country's stability and sovereignty. The Russian invasion of Ukraine serves as a catalyst for such narratives, as it fuels perceptions of a global power struggle with ramifications for Egypt and the wider Middle East.

Social Media Affordances for Authoritarian Regimes to Spread Conspiracy Theories

Social media had provided a great opportunity for authoritarian regimes to create an affective propaganda machine and to silence the opposition by demonising them and taking over the only space available for them. The pro-government propaganda has been greatly amplified by the extensive use of digital technologies across a range of social media platforms, with the emergence of Facebook, Twitter, TikTok, and YouTube, as well as online television networks and various websites as prominent means of disseminating them. These platforms played a pivotal role in amplifying and circulating

narratives, reaching a wide and diverse audience online. This has had a profound impact on ordinary individuals, as evidenced by widespread engagement through comments, shares, and likes on social media posts. Reactions to the pro-government conspiracy theories among the general public are particularly significant, indicating the significant influence of such narratives within society. A key element of this process involves deploying bots and robots to amplify the reach and impact of the pro-government propaganda including the spread of pro-government conspiracy narratives.

Similarly, social media has provided key affordances to the Egyptian regimes in propagating the aforementioned conspiracy theories. Importantly, platforms such as YouTube and Facebook allowed the regime to not only reach younger, more tech-savvy demographics but also implicate their Western "partners" in such conspiracy theories without naming them in official language. This was in line with Theocharis et al.'s (2023) finding that YouTube and Facebook have a positive effect on conspiracy beliefs.

Conspiracy narratives have been spread through social media accounts linked to a group of influential young journalists and YouTube personalities who have actively supported President Sisi's regime for years. Among the most prominent figures are Sherif Elsirfy, Ahmed Mubarak, and Mohamed Kandeil, all of whom gained prominence in the media terrain after Sisi took power in 2013. Through their online platforms, they have consistently produced and shared pro-government content, reinforcing and amplifying narratives that align with the administration. Their digital influence has played a key role in shaping public discourse and widening the reach of conspiracy theories.

Elsirfy has over a million subscribers on YouTube, actively publishing pro-Sisi content on Twitter, Facebook, and TikTok. Ahmed Mubarak is another media activist with over 1.7 million followers on his Facebook page and about 300,000 subscribers on YouTube. Mohamed Kandeil has over half a million subscribers on his YouTube. They all have been actively supporting the Sisi government during the last few years and have huge numbers of followers even though they lack any professional background in media or politics.

Numerous pro-government propagandists have harnessed the power of YouTube as a primary medium for creating and disseminating an array of conspiracy narratives aimed at bolstering the Egyptian government's image, with a particular focus on President Sisi. Ahmed Mubarak stands out as one of the most prolific YouTubers, having posted 1,000 videos over the past seven years with 290,000 subscribers. He also has a Facebook account, sharing his content there as well. Many of his video productions are dedicated to advancing conspiracy theories that serve the interests of the Egyptian government. Notably, one of his lengthier video presentations, in which he expounds on the conspiracy surrounding Egypt's withdrawal from the Grains

agreement, has garnered significant attention (Mubarak 2023a). With a compelling title that hints at conspiratorial undertones, the video is designed to capture the audience's imagination. Titled "Urgent and Dangerous! Russian Intelligence Reveals a Conspiracy Against Egypt, and Sisi Calls Putin to Thank Him and Withdraw from the Wheat Agreement!" this video has amassed a remarkable 151,000 views, 6,200 likes, and 583 comments, showcasing the effectiveness of his approach in engaging and resonating with a wide viewership. Mohamed Kandeil emerges as another prominent pro-government propagandist, boasting an extensive portfolio of 3,600 videos and an impressive subscriber base of 534,000 individuals. Among his video content, one video discusses the conspiracy theory surrounding Egypt's withdrawal from the grain agreement, intriguingly titled "Egypt's Withdrawal Changes the Power Balance" (Kandeil 2023). The title alludes to the narrative's appeal and ability to resonate with a sizeable viewership.

John Elmasry (2023a) is yet another notable pro-government YouTuber, boasting a substantial library of 940 videos and a considerable following of 500,000 subscribers. His content primarily concerns promoting the Egyptian government and President Sisi, frequently employing conspiracy theories to advance his narratives. This large amount of reach and engagement is raising serious questions due to the recent establishment of the account in September 2019. It has affiliated accounts on Facebook, Twitter, and TikTok. In one of his more extended videos, an 18-minute presentation discussing the conspiracy theory of an economic war on Egypt, he linked the conspiracy to the US Federal Reserve and the International Monetary Fund (IMF), accusing the US of a conspiracy against Egypt (Elmasry 2023b). In another video, Elmasry (2023c) attributed a role to the Muslim Brotherhood in the Western economic war against Egypt by planning to withdraw $4 billion from the Egyptian market to weaken the Sisi government. These figures underscore the efficacy of his approach in captivating a substantial online audience and disseminating his perspectives on Egypt's political terrain. In another video titled "Zelensky is coming to rule Egypt," John Elmasry warns about the emergence of civil candidates challenging President Sisi in the upcoming Egyptian elections. He portrays these candidates as a significant threat to Egypt's national interests, suggesting their rise could lead to the country's descent into chaos. Additionally, the video highlights President Sisi's achievements in stabilising the Egyptian pound despite alleged conspiracies to overthrow his rule.

This shift in the approach of authoritarian regimes toward social media highlights a significant transformation in their strategies. While they initially attempted to restrict, block, or control these platforms, they have now evolved to exploit them as powerful tools for their own purposes. This transformation is not limited to a specific region but is observed globally, as seen in the case of Russia and other countries. Egypt, particularly after the Sisi coup, exemplifies this trend, as noted by Amr Magdi, an Egyptian researcher

and activist. In his interview, Magdi claimed that authoritarian regimes have recognised the potential of social media for advancing their agendas and have strategically penetrated these platforms to achieve their goals. Over the past seven years, they have cultivated their own armies of online actors, including trolls and inauthentic accounts, which they deploy in various forms. Magdi said,

> This extensive presence of government-backed online forces has made it increasingly challenging for individuals and movements to effectively mobilize on social media, as the terrain is now inundated with thousands of such accounts. This paradigm shift underscores the significance of understanding how these regimes leverage digital technologies and manipulate social media to maintain their authority and control over their societies.

What makes the regimes more powerful than the opposition or independent actors in social media is that the regimes have much large resources to use social media relative to the others. Magdi explains that:

> The government or pro-government agencies can be online eight to 12 hours a day just to amplify the government message and opinion about things, and the other form is adjusted electronic auto bot. So, the authoritarian governments have mastered and manipulated these platforms, and unfortunately, these platforms have not risen up or developed their tools to technical these issues as they should have known because, unfortunately, they are more concerned about their profits and growing their numbers of users on their platforms more than anything else.

In an interview, an Egyptian researcher and activist, who requested anonymity, emphasised how the regime demonises the opposition by labeling them as terrorists and enemies of the state. He noted that the Egyptian government has long focused on suppressing the Muslim Brotherhood and combating perceived fundamentalism and extremism. This has primarily served as a pretext to stifle freedom of speech, the right to protest, and press freedom. His insights highlight the need to examine how authoritarian regimes leverage digital technologies and other tools to shape narratives, silence dissent, and influence both national and global perceptions. These tactics not only impact domestic politics but also carry significant diplomatic, political, and economic consequences on the international stage.

After analyzing hundreds of comments on pro-government conspiracy theories in social media, the diverse range and substantial quantity of these comments stand out. From expressions of praise for Egypt, the government, the army, the intelligence institution, and President Sisi, to outright attacks on the opposition and its leaders, along with extensive sharing and reposting,

the propaganda machine proves to be effective with profound and extensive impact on Egyptian society, affecting both ordinary citizens and the elite. This shows that social media have evolved into a potent tool for the government, enabling the maintenance of power, manipulation of public sentiment, and suppression of opposition forces.

History and Cultural Background

Conspiracy theories that gain prevalence in a society function as tools to reinforce the established values of an in-group and serve to identify and negatively portray outsiders, influenced by social, historical, or geographical context (see Nyhan and Zeitzoff 2018). The reception of a given conspiracy theory varies among different groups due to differences in collective imagination, collective memory, biases, and stereotypes. Consequently, this inclination is heightened when conspiracy theories implicate political opponents (Byford 2011).

Therefore, to understand these contemporary narratives, one must look into the historical events that paved the way for their emergence. The Arab Spring, the rule of the Muslim Brotherhood, and the 2013 coup serve as pivotal points. Arab Spring was supported and encouraged strongly by the West, which led to the rule of the Muslim Brotherhood, which is seen as a group backed by the US and the West in general in Egypt. The chaos that resulted from the Arab Spring and Muslim Brotherhood rule paved the ground for public support of the 2013 coup and the return to dictatorship. This provided support for public acceptance of Western conspiracy theories against Egypt (Koehler-Derrick et al. 2017).

The roots of such conspiracy theories extend further into Western colonialism in general, and US interventions in the Muslim world in particular, including Iraq and Afghanistan, and supporting Israel against Palestine, not to mention Ukraine as a recent example outside of the Muslim World. These actions have generated widespread skepticism and mistrust, providing fertile ground for cultivating anti-American conspiracy narratives (Gray 2010a). Conversely, Russia, particularly under the leadership of Vladimir Putin, has repositioned itself within the Middle East as a robust and influential player that counters the will of the US. This strategic shift has altered the regional perception of Russia, depicting it as a nation that defies American dominance. The ongoing conflict between Russia and its Western allies, particularly in the context of the war in Ukraine, has reinforced this image of Russia as a formidable force challenging the US interests.

Conspiracy Theories: Connecting Bread and Geopolitics in Egypt

By linking economic hardships to Western conspiracies, Egyptian propaganda diverts public frustration away from domestic policies, reinforcing national

unity around President Sisi's leadership. This part explores how these theories emerge, their geopolitical implications, and the role of social media in amplifying them.

Russia's Alleged Role in Egypt's Withdrawal From the International Grains Agreement

Amid the Ukraine war and Egypt's worsening food crisis, the government announced in March 2023 its withdrawal from the International Grains Agreement (IGA), effective July. The agreement, involving 35 member states, aimed to secure global grain trade. As one of the world's largest wheat importers (12 million tons annually), Egypt faced massive challenges due to the crisis, including reduced wheat supplies, increased prices, decreased tourism revenue, and a foreign currency shortage, causing a significant depreciation of the Egyptian pound. According to the Egyptian government, the Grains Agreement, however, failed to provide any support to Egypt (Tanchum 2023), leading to its decision to withdraw from the agreement and enter into a bilateral agreement with Russia. However, pro-government narratives turned this decision into a conspiracy theory, portraying Sisi as a national hero and claiming Russia thwarted a US plot to destabilise Egypt through grain shortages.

While Egypt's decision to exit the agreement was grounded in economic concerns (Lewis and El Safety 2023), specifically the food crisis triggered by the Ukrainian war, this theory spun a different narrative. As articulated by a popular pro-government internet personality Ahmed Mubarak (2023a) in a YouTube video titled "Russian Intelligence Service Reveal a Conspiracy," the narrative argued that as the war in Ukraine was ongoing, the US planned to exploit the food crisis in Egypt to foment chaos, trigger a hunger-driven revolution, and destabilise the region. This, in turn, would serve as a pretext for renewed US intervention in the region, potentially opening new fronts against Russia. Counteracting the conspiracy, Russian intelligence allegedly provided critical information to Egyptian authorities, prompting their withdrawal from the agreement. According to Mubarak (2023a), "The Russian embassy in Cairo published the terms of an American and European conspiracy against the Egyptians that aimed at turning them against their president." Egypt subsequently secured its grain supply directly from Russia at a competitive price and in sufficient quantities, amounting to 8 billion tons of its annual 12-billion-ton grain import. To make the conspiracy more realistic, the story was linked to a phone call between Sisi and Putin, claiming that the Russian move was gratified by President Sisi, who personally thanked Russian President Putin for saving Egypt from the crisis in a phone call (Mubarak 2023a).

Russia capitalised on the global food crisis to enhance its image in Africa by delivering on President Vladimir Putin's promise to provide free grains to

six African countries, a commitment fulfilled since November 2023 (Reuters 2023). Additionally, Russia competitively priced the grains supplied to Egypt, meeting the country's requirements. This strategic maneuver positioned Russia as a crisis-supporting benefactor and showcased its capacity to exploit situations for geopolitical and economic advantages. The Russian Embassy in Cairo officially announced its commitment to ensuring food security for Egypt after the deal, emphasising Russia's ongoing role as a significant supplier of agricultural products to the country (RT Arabic 2023a). This announcement highlights the diplomatic and economic consequences of the bilateral agreement, confirming Russia's role as a key partner in addressing Egypt's agricultural needs.

Egyptian officials also welcomed the move toward Russia, considering it a defensive action against Western domination of Egypt. Major General Khairat Shukri, Undersecretary of State Security Investigations, offered his perspective on Egypt's withdrawal from the Grain Agreement, asserting that the country's membership in the agreement does not bring "added value" (RT Arabic 2023b). He highlighted that, in his view, the decision marks the commencement of acquiring hard currency, with Egypt opting to conduct transactions with Russia (the primary exporter) and India for wheat and grains in Egyptian pounds based on mutual agreements. Shukri emphasised that Egypt's decision is robust across all aspects, positioning it as a proactive measure toward reform and a move that challenges the dominance of the dollar in such transactions.

Economic War Against Egypt

Another conspiracy narrative that has become prevalent in recent years is related to the ongoing economic crisis in Egypt. The country's economic situation has been getting worse since al-Sisi's takeover in 2013, which forced the government to seek a bailout package from the IMF in 2016. In November 2016, the IMF and Egypt signed a $12 billion loan agreement with the aim of "addressing macroeconomic vulnerabilities and promoting inclusive growth and job creation" (Momani 2018). Prior to the IMF program, these vulnerabilities included an overvalued exchange rate (and the corresponding rise of a parallel, or black market, exchange rate); foreign exchange scarcity, which severely undermined private-sector activity; a dramatic drop in foreign exchange reserves; large fiscal deficits; and a high level of public debt.

Despite the fact that it was the Egyptian government itself who sought the bailout package from the IMF, an anti-Western conspiracy narrative has emerged in pro-government media to paint the government as the target of a major economic warfare. The narrative of economic conspiracy in Egypt is a common theory raised frequently following any economic crisis to remove

the responsibility from the government and point the blame on foreign enemies. As an example, Khaled Salah, director of a pro-Sisi platform "Youm7," claimed in 2016 (Badroddin 2016), when the Egyptian currency significantly fell that:

> Egypt was exposed to the dirtiest economic war in history to overthrow President Sisi and bring Egypt to its knees. The goal now, in the Western world, is to bring Egypt to its knees as a punishment for the independence of the Egyptians' national decision.

Such conspiracy theories intensified in 2023 when the economic situation turned from dire to catastrophic due to the Russian invasion of Ukraine and subsequent crises in energy and grain markets (Tanchum 2023). The Egyptian government approached the International Monetary Fund (IMF) once again for a $3 billion loan. IMF required some economic measures from Egypt, affecting citizens' economic lives. The country has already been suffering from ineffective economic governance, which has failed to address the country's economic crisis over decades. In such an environment, a compelling conspiracy theory has emerged within pro-government media circles, attributing Egypt's economic problems to attacks against the Egyptian economy.

We found that while the officials abstained from naming the IMF or the US as perpetrators of this alleged economic war, the pro-government journalists and online personalities have deliberately named them in their conspiracy narratives. For example, Sherif Elsirfy, a young YouTube influencer with 1.04 million subscribers, published a video in 2023 after his meeting with Sisi, quoting him, "There are external parties that put pressure on Egypt and work to float Egyptian Pound." Elsirfy (2023) clarified that Sisi is referring to the International Monetary Fund (IMF) by claiming that "Sisi rejected IMF pressure and the floating of the Egyptian pound." He has published several other videos after and before the meeting slamming the IMF for its negative role on Egypt's economy and praising Sisi for his wisdom and resistance against the IMF pressures.

This discrepancy between the official and unofficial discourse emerged due to the double bind that the Egyptian government has caught itself in its economic approach. While the regime praises the IMF and cooperation with it as being fruitful, it also orders its unofficial elements in the media to promote an anti-Western and anti-IMF economic conspiracy. For example, in a recent meeting with Managing Director of the IMF Kristalina Georgieva, Sisi stated his "appreciation" of the "constructive and fruitful cooperation between Egypt and the IMF" and declared that his government is "keen on pursuing the structural reforms pertaining to financial and monetary policy" (Egypt Today 2023b). While this was happening, the pro-government media and YouTube channels were pushing a conspiracy narrative that painted the

IMF and other Western countries and institutions as sinister actors behind a massive economic attack against Egypt. For example, the National Media Authority, which is a governmental body in Egypt, published a report attributing the crisis to a conspiracy against Egypt run by the US following the US failure to destroy Egypt in cooperation with political Islam and the Muslim Brotherhood. The author declared that "After America was shocked by the fall of the Brotherhood, they tried to paralyze Egypt's political and economic abilities" (Abdulaziz 2023).

Turning Egypt Into an Unstable Country Like Ukraine

In the light of upcoming presidential elections in Egypt, the Ukraine crisis has been used again for a conspiracy narrative against civilian candidates who intend to run for the presidential elections. The narrative is framed as a Western conspiracy to turn Egypt into a Ukraine model by fomenting instability, potentially destabilising the nation and its patriotic military leadership. Renowned within pro-government circles, Egyptian social media activist John Elmasry (2023a) has depicted the rise of civil candidates in the upcoming Egyptian elections as a harbinger of a potentially dire parallel scenario. Drawing an analogy to Ukraine's experience with Russia, Elmasry posits that:

> These emerging figures might serve as conduits for upheaval akin to that seen during the Zelensky era [in Ukraine].

His assertion evokes the narrative of Ukraine's political dynamics intertwined with Russia's influence, insinuating a potentially unsettling outcome for Egypt's political terrain. The narrative is linked to the crisis surrounding Egypt in neighboring countries like Libya, Sudan, and other African countries. Accordingly, the rise of any civilian candidate is portrayed as undermining the Egyptian army. Any alternative to the current regime would be seen as a risk to the nation as it would open the door to chaos and instability. This line was followed by Ahmed Mubarak, another famous pro-regime YouTube personality. In one of his videos, Mubarak (2023b) claimed that:

> O Egyptian people, you are now living in the atmosphere of 2013, literally, or worse. Just replace Mohamed Morsi and put in his place the secret candidate of the organization [the Muslim Brotherhood], Ahmed Tantawi, who is "Mohamed Morsi 2023." He's a new test. So, protect your country and adhere to your leadership. May God protect Egypt from All evil.

It seems that public and governmental opinion toward Russia is becoming more favorable after the Ukrainian crisis and mounting frustration with the

policies of the US and the West in general in the Middle East. This trend can be observed in the discourse of high-ranking officials as well. For example, the former director of the National Defense College and current advisor to the Egyptian military, Major General Muhammad Al-Ghobari, claimed that "Russia played an important and major role in thwarting the Greater Middle East plan that the United States of America was working to implement in the region, but Russia stopped it by standing by Syria." He argued that

> with the Russian military operation in Ukraine, Western countries put pressure on Egypt to prevent Russian ships from crossing the Suez Canal and imposed significant economic sanctions on dealing with some Russian companies and forces. Egypt circumvented this matter due to the presence of common interests with Russia.

He stressed that "Egypt and Russia are closely linked in confronting and resisting the West's conspiracy, which further strengthens cooperation between the two countries."

Strategic Deployment of Conspiracy Theories in Egypt

The three conspiracy theories that we discussed previously are part of a larger narrative around the politics of authoritarianism in Egypt, not only rooted in the anti-Western conspiracy narrative against Egypt that is spread widely among non-official media but also promoted directly by the officials from the top positions. President Abdul Fattah al-Sisi frequently talks about conspiracies against the Arab World and Egypt in particular, thanking Egyptians who stood against these conspiracies and prevented the country from falling in the direction of Iraq, Syria, and Libya, all that were intervened by the US and other Western allies.

As an example, in a public speech in 2018 (Extra News 2023), Sisi slammed Western powers, accusing them of having ambitions and conspiracies about the region and Egypt:

> The great powers which had ambitions about the Arab wealth sought to exploit the uprisings among the people to advance extremist groups and sponsors of terrorism into positions of power. They perceived an opportunity to overthrow Arab nations, disrupt their capabilities, and sever their connections. The magnitude of these events was profound, particularly in countries like Syria, Iraq, Libya, and Yemen, and even earlier in Afghanistan and Somalia.

Sisi used the consequences of the Western role in Iraq, Syria, and Libya as a method to promote his rule in Egypt and scare Egyptians from seeking

change in their country, which would lead them to get trapped in conspiracies undertaken in other Middle Eastern countries:

> It has become increasingly evident that Egypt occupied a central role as the primary target and the most coveted prize for those with malevolent intentions. The awareness and vigilance of the Egyptian people, who had been prepared to defend their homeland, played a crucial role in thwarting the schemes of those who sought to undermine the country.
>
> *(Extra News 2023)*

Prime Minister Mostafa Madbouly frequently speaks about media conspiracy against Egypt. In a public speech last year, he said (Abulfadl 2022):

> We have observed 150 articles in paid-for newspapers and international websites, all working in line with the series of foreign conspiracies, portraying Egypt in a negative picture.

Triggering fear among the citizens to make them stick to the current government is a common way that even Egyptian officials use to scare people from any changes, raising the potential fear of conspiracy against Egypt. This discourse usually intensifies as the country gets closer to the election time. In a public speech last March, President Sisi warned Egyptians about the consequences of popular anger over the deteriorating economic situation in the country, saying (Egypt Today 2023a):

> Be aware and beware of this matter being repeated. Be aware, O Egyptians, that you are once again causing the ruin of your country. Anger over economic difficulties and protesting for change were used when the country collapsed in 2011.

While Sisi's words are not explicit in naming the foreign perpetrators, other bureaucrats and social media personalities explicitly refer to the West as the main perpetrator of conspiracies against Egypt. Following the European Union's statement this October criticising Egypt for silencing the opposition and not allowing them to participate in the elections, several Egyptian officials slammed the European Union, accusing it of seeking chaos in Egypt. Major General Ibrahim Al-Masry, Undersecretary of the Defence and National Security Committee in the House of Representatives, said (Yousef 2023): "The European Parliament's allegations aim to destabilize Egypt."

In authoritarian regimes, conspiracy theories are vital for consolidating and justifying power by directing public dissatisfaction toward perceived formidable enemies (Giry and Gurpinar 2020; Madison and Ventsel 2020). The Egyptian propaganda machine employs a dual strategy to shape public

perception of the current regime. Defensively, it portrays the regime as legitimate and patriotic, emphasising adherence to legal frameworks and framing actions as essential for national well-being. Leaders are depicted heroically, and the system they lead is flawless. Offensively, it discredits alternatives, labeling opposition as traitors, criminals, or foreign agents. Conspiracy theories link opposition to nefarious plots or foreign interference, undermining opposing narratives. National unity sentiments are manipulated to marginalise dissent, framing the regime as a unifying force and opposition as divisive threats. This approach aims to fortify public support while diminishing dissenting voices, blending defensive and offensive tactics seamlessly. It reinforces the regime's image, marginalising alternatives and fostering public trust and unity.

Like many examples Igor Golomstock provided in his book Totalitarian Art (1990), Egyptian propaganda presents the head of state as the father of the nation, and any attempt to criticise him or his authority is introduced as a betrayal of Egypt. Egyptian TV channels frequently host Arab leaders praising Sisi and portraying him as the savior of Egypt and the Arab nation. In an interview with CBC Egypt (2014), the president of the State of Palestine, Mahmoud Abbas, said: "The Arab nation must support Sisi because he saved Egypt and the Arab and Islamic nations from ages of darkness."

In the same context, and with a populistic tendency, the president's image is portrayed as a "Man of action, not words." The slogan "Man of actions, not words" has been used broadly in social media, news websites, and TV channels in many different ways. In conjunction with the magnification and glorification of the president's image, extensive work has been done to demonise the image of the opposition as a whole, generalising all under the unsightly titles of "traitors" cooperating with foreign enemies, "terrorism," "riot," and "suspicious calls," slamming all attempts at demonstrations or criticising the government. As Sisi puts it:

> There are attempts to cast doubt on our achievements. The goal of these attempts is to weaken doubt in the homeland, not to serve its interests. [Whereas] the aim of the actions we take is in the interest of the Egyptian state and its people.
>
> *(Jaber 2020)*

Manipulative tactics have also been used broadly to shape public opinion in favor of the state and the head of it. These tactics aim to form a fake picture of the political system to be seen as democratic but, in fact, under full control of the authoritarian leader with no possibility of form or change. This takes place by eliminating serious contenders and creating a facade of competition in the presidential election, which has been used constantly in all previous elections. For example, following the announcements of credible

candidates in 2018, such as Khaled Ali, Ahmed Shafik, and Lieutenant General Sami Anan, they were systematically purged from the race (Hassanein 2018). Shafik was reportedly coerced into withdrawal through detention, compelled to praise Sisi's leadership. Anan faced dubious charges and was imprisoned upon declaring his candidacy. Other potential candidates, including the nephew of former President Anwar Sadat and leftist activist Khaled Ali, were either pressured not to run or subjected to harassment by security forces. The sole remaining candidate, Moussa Mustafa Moussa, is portrayed as a pseudo-opponent, having registered at the last minute with a history of endorsing Sisi on social media, highlighting the orchestrated nature of the electoral process under Sisi's regime. Similarly, in 2023, supporters of those intending to run against President Sisi were prevented from registering their support to enable their candidate to become an official candidate (Saleh 2023). Candidates must collect notarised authorisations from 25,000 citizens in 15 governorates of the country. Alternatively, they could submit the approval of 20 members of parliament, but the council is overwhelmingly made up of Sisi loyalists. The remaining candidates, head of the Liberal Wafd Party Abdel-Sanad Yamama, chairman of the Republican People's Party Hazem Omar, and head of the Egyptian Democratic Party Farid Zahran are all supporters of Sisi and are not considered competitive to him.

Conclusion

This chapter examined three prevalent conspiracy narratives in Egypt: a significant yet understudied case from the Global South related to its withdrawal from the International Grains Agreement, an alleged economic war against Egypt, and alleged Western attempts to destabilise the country since the 2013 coup. The study revealed how social media, especially through influential internet personalities, provided the authoritarian regime with a platform to disseminate these narratives widely, targeting a younger, tech-savvy audience. These conspiracy theories implicated official partners like the US and the International Monetary Fund (IMF) directly and indirectly depending on the speaker's official status.

We showed Egypt's historical experiences, including periods of colonialism, military interventions, and geopolitical rivalries, provide fertile ground for the proliferation of conspiracy theories that portray external actors as malevolent forces seeking to undermine the country's stability and sovereignty. These conspiracy theories have been a part of a broader authoritarian narrative in Egypt, promoted not only by non-official figures but also by high-ranking officials. The Egyptian propaganda machine adopted a dual strategy. Defensively, it portrayed the regime as legitimate and patriotic, emphasising adherence to legal frameworks and framing actions as essential for national well-being. Offensively, it discredited any alternative to the

current regime. The findings presented in this chapter offer valuable insights into the dynamics of social media, conspiracy theories, and authoritarian politics in Egypt. Future research may examine other cases to see how the findings travel. This may involve identifying prevalent conspiracy theories within these contexts, analyzing their origins and development, and examining the role of social media platforms in their dissemination.

Funding: This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.

References

Abdulaziz, Ibrahim. (2023). Inspired by the June 30 Revolution: The Brotherhood, with their political stupidity, foiled the conspiracy against Egypt. *Maspero*. https://bit.ly/48Tf9u3

Abulfadl, Muhamyoumad. (2022). The conspiracy against Egypt again. *Al-Arab News*. https://bit.ly/3vqZ5kL

Badroddin, Maryam. (2016). The great conspiracy. Khaled Salah reveals: Egypt is exposed to the dirtiest economic war in history. *Parlmany*. https://bit.ly/3vc8pbQ

Byford, J. (2011). *Conspiracy theories: A critical introduction*. Springer.

CBC Egypt. (2014). Abu Mazen: The Arab nation must support Sisi because he saved Egypt from darkness at the risk of his life. *YouTube*. https://www.youtube.com/watch?v=YCSPHLmsKXw

Cinelli, M., Etta, G., Avalle, M., . . . Quattrociocchi, W. (2022). Conspiracy theories and social media platforms. *Current Opinion in Psychology*, 101407.

Clarke, S. (2007). Conspiracy theories and the Internet: Controlled demolition and arrested development. *Episteme*, *4*(2), 167–180.

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S. & Deravi, F. (2019). Understanding conspiracy theories. *Political Psychology*, *40*, 3–35.

Egypt Today. (2023a). Sisi: 2011–2013 instability depleted Egyptian state; Nations need security and stability to progress. *Egypt Today*, October 1. https://www.egypttoday.com/Article/1/127320/Sisi-2011-2013-instability-depleted-Egyptian-state-Nations-need-security

Egypt Today. (2023b). Sisi appreciates constructive cooperation between Egypt, IMF implementing economic reform. https://www.egypttoday.com/Article/1/122514/Sisi-appreciates-constructive-cooperation-between-Egypt-IMF-implementing-economic-reform

Elmasry, John. (2023a). Zelensky is coming to rule Egypt. The Egyptian pound is rising despite the conspiracy to overthrow Sisi's rule. *YouTube*. https://www.youtube.com/watch?v=5m3XKECfHFQ

Elmasry, John. (2023b). The pound rises against the dollar, and the US Federal Reserve is passionate about the Egyptian economy. *YouTube*. https://www.youtube.com/watch?v=neaCg0CLZCk

Elmasry, John. (2023c). Al-Sisi has officially driven the people mad with high prices. *YouTube*. https://www.youtube.com/watch?v=jAV41Lq6iec

Elsirfy, Sherif. (2023). Al-Sisi rejects the flotation of the pound and the pressures of the International Monetary Fund. *YouTube*. https://www.youtube.com/watch?v=K1pPVknUEvo

Extra News. (2023). *Sisi: The awareness of the great Egyptian people was behind thwarting the conspiracies against my country*. https://www.youtube.com/watch?v=8KAW9BtWlIU

Giry, J. & Gürpınar, D. (2020). Functions and uses of conspiracy theories in authoritarian regimes. In M. Butter & P. Knight (Eds.), *Routledge Handbook of Conspiracy Theories*. Graz, Austria: Institute of Public Law and Political Science.

Gray, M. (2010a). *Conspiracy theories in the Arab world: Sources and politics*. Routledge.

Gray, M. (2010b). Revisiting Saddam Hussein's political language: The sources and roles of conspiracy theories. *Arab Studies Quarterly*, *32*(1), 28–46.

Hassanein, Haisam. (2018). President Trump, Condemn this Sham Egyptian election. *The Washington Institute*. https://www.washingtoninstitute.org/policy-analysis/president-trump-condemn-sham-egyptian-election

Jaber, Ibrahim. (2020). Al-Sisi and the sceptics: The state's challenges and projects are the fuel for responding to suspicious calls. *Roayah News*. https://bit.ly/3TUohdn

Kandeil, Mohamed. (2023). Egypt's withdrawal changes the power balance. *YouTube*. https://www.youtube.com/watch?v=N_s42wJ8fTk

Koehler-Derrick, G., Nielsen, R. A. & D. Romney. (2017). *Conspiracy theories in the Egyptian State-Controlled Press*, unpublished manuscript. https://scholar.harvard.edu/files/gkd/files/conspiracy_10april2017_aalims.pdf.

Lewis, Aidan & Sarah El Safety. (2023). Egypt withdraws from UN grain treaty prompting sadness and concern. *Reuters*. https://www.reuters.com/markets/commodities/egypt-withdraws-un-grain-treaty-prompting-sadness-concern-2023-03-09/

Madison, M. L. & Ventsel, A. (2020). *Strategic conspiracy narratives: A semiotic approach*. Routledge.

Mahl, D., Schäfer, M. S. & Zeng, J. (2023). Conspiracy theories in online environments: An interdisciplinary literature review and agenda for future research. *New Media & Society*, *25*(7), 1781–1801.

Marczak, Bill, John Scott-Railton, Daniel Roethlisberger, . . . Ron Deibert. Predator in the wires. *Citizen Lab*. https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

Momani, Bessma. (2018). Egypt's IMF program: Assessing the political economy challenges. *Brookings Institute*. https://www.brookings.edu/articles/egypts-imf-program-assessing-the-political-economy-challenges/

Mubarak, Ahmed. (2023a) Russian intelligence service reveal a conspiracy. *YouTube*. https://www.youtube.com/watch?v=feGS1nhyg2s

Mubarak, Ahmed. (2023b). Al-Sisi reveals the Brotherhood's plan to create a mob to burn the administrative capital during the presidential elections!. *YouTube*. https://www.youtube.com/watch?v=v7XE985LmNs

Nyhan, B. & Zeitzoff, T. (2018). Conspiracy and misperception belief in the Middle East and North Africa. *The Journal of Politics*, *80*(4), 1400–1404.

Reuters. (2023). *Russia says first free grain shipments to Africa are on their way*. https://www.reuters.com/markets/commodities/russia-begins-supplying-free-grain-african-countries-agriculture-minister-2023-11-17/

RT Arabic. (2023a). *Security expert appreciates Egypt's withdrawal from the grain agreement, considers it a severe blow to the dollar*. https://bit.ly/41NB2bM

RT Arabic. (2023b). *Wheat to Egypt . . . between bids and reality*. https://bit.ly/3NV1JW3

Saleh, Heba. (2023). Egypt candidates claim intimidation is being used to stifle opposition vote. *Financial Times*. https://www.ft.com/content/9f91731b-c9f8–4148-aecf-e904adb24c6f

Sunstein, C. R. & Vermeule, A. (2009). Conspiracy theories: Causes and cures. *Journal of Political Philosophy*, *17*(2), 202–227.

Tanchum, Michaël. 2023, July 25. The Russia-Ukraine war forces Egypt to face the need to feed itself. *Middle East Institute*. https://www.mei.edu/publications/russia-ukraine-war-forces-egypt-face-need-feed-itself-infrastructure-international

Theocharis, Y., Cardenal, A., Jin, . . . Štětka, V. (2023). Does the platform matter? Social media and COVID-19 conspiracy theory beliefs in 17 countries. *New Media & Society*, *25*(12), 3412–3437.

Yousef, Mohamed. (2023). Parliament's Defense Committee: The European Parliament's allegations aim to destabilize Egypt. *El Watan News*. https://www.elwatannews.com/news/details/6848953

Zonis, M. & Joseph, C. M. (1994). Conspiracy thinking in the Middle East. *Political Psychology*, 443–459.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

PART 3

Digital Authoritarianism

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

6

#PROPAGANDA: MANUFACTURING CONSENT THROUGH STATE ACTORS' SDIOs IN THAILAND

Itsakul Unahakate

Introduction

In March 2021, Facebook Inc. (now Meta Platform Inc.) announced that it had taken down 185 Thai accounts with ties to the government as part of an information operation in the country sponsored by the military. The company stated that "[t]his is the first time that we've attributed one of our takedowns to links to the Thai military" (Tanakasempipat 2021). This is, however, not the first time that there is evidence that the Royal Thai Army (RTA) has been involved in the so-called Strategic Digital Information Operations (SDIOs). Back in October 2020, Twitter suspended 926 accounts after investigating that these pro-RTA accounts had engaged in behavior targeting key political opposition figures (News Agencies and Post Reporters 2020).

According to the Stanford Internet Observatory, the military-linked Twitter network had limited influence (Goldstein et al. 2020). However, targeted individuals and groups may disagree. The program manager of iLaw, a Thailand's human rights and legal watchdog, argues that the Thai military has well-coordinated networks, systematically sharing and reposting specific content to change people's attitudes (Asia Centre 2023). These networks consist of pro-regime media outlets and royalist civic groups, which are motivated by ideology to protect the monarchy (Sombatpoonsiri 2022).

So, how can we assess whether the army's SDIOs have an impact? This chapter argues that in order to assess its influence, it is necessary to comprehend the dynamic nature of SDIOs, including not only the actors but also their interactions with the changing environment, especially communication systems. This chapter, then, examines the political economy of SDIOs in Thailand by revisiting the Propaganda Model proposed by Edward S.

DOI: 10.4324/9781003628088-9
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

Herman and Noam Chomsky (Herman and Chomsky 2002). It first starts with a brief background over the past decade. The second section provides an explanation of the dynamics of SDIOs, especially those organised by the Army. The third section applies the Propaganda Model to analyze the SDIOs by state and non-state actors in a broader context. The final section presents the conclusion.

Background

Thailand saw a period of political upheaval in the past decade. In 2014, Thailand experienced its second coup d'état within a span of just eight years. The country was then governed by a military junta called the National Council for Peace and Order (NCPO) until 2019, when a general election was held. General Prayut Chan-o-cha, the leader of the NCPO and later the candidate for the Prime Minister from Palang Pracharath Party (PPRP), prolonged his tenure in the prime minister's office for another four years due to interim provisions in the Constitution of the Kingdom BE 2560 (2017) allowing NCPO-appointed senators to vote for the prime minister (McCargo and Alexander 2019).

Before the 2019 general election, the Future Forward Party (FFP) was perceived by the political establishment as nothing more than a fringe party. However, Thanathorn Juangroongruangkit, the leader and the prime ministerial candidate of the party, experienced a surge in popularity, particularly among the young voters, throughout the election campaign on both social media platforms and offline. This posed a challenge to those pro-establishment forces who backed Prime Minister Prayut (Goldstein et al. 2020). In the event the FFP was unable to form a government and instead joined Pheu Thai Party in the opposition following the election, General Apirat Kongsompong, RTA Chief at the time, stated in an interview in August 2019 that "[s]ome political parties, just born a couple of years ago. [These parties] had the platform of their propaganda directed to [people] when they were 16 and 17. [They] try to educate them with fake news" (Johnson et al. 2019).

The FFP's dissolution in early 2020 sparked anger, especially among youth and students, leading to the first wave of youth protests. Initially held as flash mobs on campuses, protests took to the streets as universities closed due to COVID-19, with numbers growing. Protesters issued three key demands: an end to intimidation, parliament's dissolution, and a new constitution. The military-backed government responded with violence, including arrests and tear gas (Lertchoosakul 2021). Indeed, social media platforms, particularly Twitter (now X), again, played a key role in facilitating the youth and mobilising the protest, with popular hashtags like #FreeYouth, #เด็กเลว (#badstudent), and #เลิกเรียนแล้วไปกระทรวง (#AfterSchoolLetsGototheMinistry) (Sinpeng 2021). Eventually, following nearly nine years of unrest under General Prayut's leadership, Thailand held another general election in May 2023,

following. Unlike past elections in which social media was used as a political campaign tool, this was arguably the first time that social media had a significant impact on election outcomes (Sinpeng 2024).

This decade of political turmoil has, undoubtedly, coincided with a period of substantial transformation in communication. The widespread and rapid adoption of the Internet and social media in Thailand has changed interpersonal communication and interaction. Statistics indicate that the prevalence of social media usage has continuously risen over the last ten years. According to the most recent report in early 2024, Thais spent an average of over eight hours on the Internet daily, with two and a half hours allocated to social media. The top social media platforms are LINE, Facebook, TikTok, and YouTube, with 54.0 million, 49.1 million, 44.38 million, and 44.2 million members, respectively (Kemp 2020). While media outlets remain the primary source of news for Thai people, the younger they are, the more they rely on other sources, especially their social media networks (Thammasat University Research and Consultancy 2020). These data suggest that traditional mass media may not remain the primary source of information for much longer.

The military has also been concerned about this tendency. A study by the National Defence Studies Institute (NDSI) under Royal Thai Armed Forces Headquarters argues:

> The power of information and media have transitioned from the state to private sector and civil society. Because of fully connected data, which enables real-time information dissemination, information and media influence people's opinions, believes and responses at national and international levels widely. This phenomenon causes telecommunication media, particularly the Internet, to influence national decisions like never before and impact the security aspect substantially.
>
> *(National Defence Studies Institute 2016, 1–2)*

This NDSI's study appears to have been the first public-access military document that discusses social media and, to some extent, represents the Thai military's perspective on the subject. It highlights the importance of developing the military's guidelines for information operation (IO) and strategic communication. The study also claims that on social media, anyone may be a media creator with little investing and without seeking content references (National Defence Studies Institute 2016). This could indicate the military's fear for alternative sources of information and its motivation to conduct IO.

Strategic Digital Information Operations in Thailand

Thailand's recent IO align with the concept of SDIOs. In Chapter 1 of this volume, Ihsan Yilmaz and Shahram Akbarzadeh use this term to refer to "deliberate, technology-enabled efforts by state and non-state actors to manipulate

the information environment, influencing both public opinion and collective emotions." The authors point out that while IO have been developed over the last century, the digital environment has brought fundamentally new and sophisticated tools, as well as the ability for more extensive dissemination and reach for strategic IO. This chapter suggests, however, that this does not always imply that state actors can adapt to the changing digital environment simultaneously. Those who attempt to shape public opinion with SDIOs may have to proceed by trial and error for a long time before settling on a more effective strategy. This is an ongoing process. In case of Thailand, recent uses of SDIOs show that these executions are dynamic. State and non-state actors are in a process of learning, adapting, and normalising SDIOs.

Learning

Although the Thai military's IO can be traced back to the counter-communism campaigns of the 1960s (Sombatpoonsiri 2022), the process of learning to conduct SDIOs is relatively new. One of the most recent noteworthy examples of how the Army conducts IO in response to internet information flow was the so-called Anti-monarchy Plot Diagram (ผังล้มเจ้า) during the 2010 Red Shirts movement which began after 2006 coup d'état. This controversial diagram presented the network of persons surrounding former Prime Minister Thaksin Shinawatra, who was deposed by the coup, and implied that the movement led by the United Front for Democracy Against Dictatorship (UDD) tried to topple the monarchy. After being sued for defamation, Colonel Sansern Kaewkamnerd, the Centre for the Resolution of the Emergency Situation (CRES) spokesperson who shared the diagram with the press,[1] later admitted to the criminal court that the diagram only depicts the relationship between the documented names and did not claim that such people were involved in the movement to overthrow the monarchy. Instead, the press made certain assumptions and magnified the diagram. He testified that one of the reasons behind the diagram was that the CRES sought to repel false information on the Internet about Queen Sirikit's political interference (Prachatai 2011). This exemplifies the Army's efforts to undermine the credibility of political oppositions (McCargo 2017).

Another example is the website pulony.blogspot.com, which spreads disinformation about the South Thailand insurgency, targeting politicians, lawyers, and activists working on human rights and labeling them as "unpatriotic traitors" (Thai Lawyers for Human Rights 2020). From 2011 to 2020, it published articles in Thai, English, Malay, and Arabic, which remain accessible today. During the motion of no confidence in February 2020, Wiroj Lakkhanaadisorn, an MP from the dissolved Future Forward Party (FFP), stated that, according to budgeting support documents, the blog was sponsored by the Internal Security Operations Command (ISOC), a unit under

the Prime Minister's Office that, in practice, remains military-controlled due to its operational structure. The ISOC spokesman eventually admitted the authenticity of the document but claimed that the funding was spent on public relations to promote a "proper understanding" of their effort to restore peace in South Thailand. He claimed that the situation was getting better, but there was a need for the blog because "the growing use of social media to propagandise, distort fact, and disseminate false information to undermine public perception, build dread and hatred through websites webpage and Facebook implicitly in many areas" (Today 2020).

Still, it was not until May 2014 that the NCPO staged a coup and announced it on social media channels, marking "the beginning of the military's digital engagement era" (Goldstein et al. 2020, 5). Regrettably, our knowledge on the military's operations under the NCPO administration is limited due to the absence of a checks and balances structure during that period. The National Legislative Assembly of Thailand, appointed by the military, had no intention to oppose the administration. However, this situation changed following the general election in 2019.

In February 2020, during the motion of no confidence, the FFP's MP Wiroj made the accusation that General Prayut, both Prime Minister and Minister of Defence at the time, was responsible for directing state-sponsored IO across multiple platforms, including the aforementioned blog, Facebook, and Twitter. These operations were evidenced by two leaked Army internal memos: one dated in April 2019, shortly after the general election, and the other in November 2019, one month following General Apirat's interview. These memos commanded the formation of operation units and provided guidelines for conducting IO, such as creating fake accounts, promoting profiles and pages on the government and military side, and undermining those of the oppositions.

The evidence was supported by Twitter's and Facebook's subsequent actions. In October 2020, Twitter took down 926 accounts after an investigation revealing that these accounts, which linked to the RTA, had actively engaged in behavior aimed at undermining opposing politicians (News Agencies and Post Reporters 2020). Similarly, in March 2021, Facebook removed 77 accounts, 72 pages, and 18 groups on Facebook, as well as 18 accounts on Instagram, for violating Facebook's policy on coordinated inauthentic behavior (CIB) – an effort to "manipulate public debate for a strategic goal where fake accounts are central to the operation" (Giglietto 2022, 281). Facebook stated that "[w]e found clear links between this operation and the Thai military's Internal Security Operations Command. We can see that all of these accounts and groups are tied together as part of this operation" (Tanakasempipat 2021).

Regarding Twitter's removal of accounts, Stanford Internet Observatory discover that most of these Twitter accounts employed similar strategies

as observed in cyber armies from other countries worldwide: creating fake accounts to conceal their identity and interest. They were created between December 2019 and January 2020, and most tweets appearing from February 2020 coincided with the period when the FFP was about to be dissolved by the Thai constitutional court. Undoubtedly, one of the main themes of their tweets was to criticise the FFP and the Move Forward Party (MFP) – the FFP's successor party. These removed accounts used vague words to attack the parties and often counter the FFP's criticisms of how the dissolution case was handled. Another notable theme was the effort to downplay criticism of military reform following the Korat mass shooting in February 2020. The incident, the worst mass shooting in Thai history, occurred in Korat when an RTA soldier stole guns from an army base and opened fire on a crowded shopping center, killing 30 civilians and injuring another 57. As a result, these accounts quickly escalated their tweets to divert attention from calls for reform and to shift blame onto the media for disseminating false information and engaging in unethical reporting (Goldstein et al. 2020).

Although there are several complicating aspects that need to be assessed, the Stanford Internet Observatory report argues that this operation had a minimal impact. These Twitter accounts received very low engagement and were unlikely to successfully distract public attention, for example, by manipulating hashtags to the extent that they become popular (Goldstein et al. 2020). However, if we take into account that this operation commenced in late 2019 when the military began to recognise the importance of social media, then this may be seen as just the opening chapter of its learning process.

Adapting

SDIOs worldwide exhibit distinct dynamics. A report by the Oxford Internet Institute suggests that:

> Over time, the primary mode for organising cyber troops has gone from involving military units that experiment with manipulating public opinion over social media networks to strategic communication firms that take contracts from governments for social media campaigns.
>
> *(Bradshaw and Howard 2017, 3)*

However, in the case of Thailand, the involvement of SDIOs has not shifted from state actors to non-state ones. Instead, they have, in parallel, adapted to the new digital environment and have been coordinated to work together in various ways. First, state actors have the ability to acquire advanced digital tools from non-state actors. In general, although state actors have a higher level of formal organisation than non-state actors, they have a lower level

of capacity. One of the reasons is that most authoritarian regimes lack the resources to develop a more sophisticated instrument (Bradshaw and Howard 2018). However, in Thailand, state actors, particularly the Army, could be an exception in this regard. While they lack the capability to develop a more advanced instrument on their own, they can acquire cutting-edge technologies with their "black budgets." An exemplary instance is the utilisation of Pegasus spyware in the surveillance of pro-democracy protesters and activists (Scott-Railton et al. 2022). In addition, they can also acquire advanced tools through their connections. In December 2020, Pannika Wanich, a former FFP MP, revealed that the Army's SDIOs used two Twitter-compatible apps to mass-post tweets. The apps, owned by a businessman with alleged ties to the military and monarchy, were provided to the Army for free. While he admitted ownership, he denied Pannika's claims and filed a complaint. The Army's spokesperson dismissed the allegations, calling them a misinterpretation of routine IO training (BBC Thai 2020).

Second, the military can leverage its networks, especially those aligned with it ideologically, to achieve broad-reaching access to targeted individuals. While the Army's IO serve as a notable illustration of state actors' SDIOs in Thailand, focusing solely on the military's operation may limit one's understanding of the broader context. In addition to organised cyber troops, there are also networks of unorganised, decentralised actors that operate from the grassroots level. These actors include pro-regime media outlets and royalist civic groups (Sombatpoonsiri 2022). The connection between the media and political movements is long-standing. This is evident in the case of partisan TV channels such as ASTV, Asia Update, and Blue Sky, which were closely associated with mass protest in the last two decades (McCargo 2017). While the media terrain has steadily shifted from mass media to social media, the pro-regime media outlets and royalist civic groups continue to play significant roles.

Pro-regime media outlets can be characterised as either a hybrid of traditional press and social media platforms, like Top News, or as wholly online social media pages, such as the *Mettad*, *Khao Sueak* (ข่าวเสือก), and The Truth. Despite having fewer page followers and engagements than anti-establishment Facebook Pages like FreeYouth (เยาวชนปลดแอก) or *Thalufah* (ทะลุฟ้า), these media outlets retain the ability to wield influence by monitoring the social media posts of the opposition and then framing their own narratives through the normative lens of royal nationalism. In doing so, they portray anti-government figures as unpatriotic and disloyal. For example, in November 2021, when there was a campaign to abolish Article 112 of the Criminal Code (the Lèse-majesté Provision), these media organisations initiated a petition using the hashtag #save112 (#ปกป้อง112) to counter the opposing hashtag #abolish112 (#ยกเลิก112). Thousands of accounts that posted the hashtag #save112 seemed to be real persons because they were different from

organised cyber troops in terms of their creation dates, account profiles, and numbers of followers. These royalists usually identified themselves as volunteer IOs or independent IOs (ไอโอจิตอาสา) (Sombatpoonsiri 2022). Many of these volunteer IOs, along with organised cyber troops, play a crucial role in digital harassment of civil society actors, particularly those who campaign for democracy or human rights. Their narratives consist of defaming someone's character and making allegations of being anti-national and engaging in sedition (Sombatpoonsiri et al. 2023).

Last, given that Thailand was in the midst of the 2023 general election, political parties appear to have a substantial influence on the evolution of SDIOs. The operations of SDIOs vary throughout political regimes around the world, but there is a common pattern. In authoritarian regimes, the modal actors are typically the state, while in democratic regimes, political parties play a central role (Bradshaw and Howard 2018). In Thailand, the line between these two actors has been increasingly blurred because of the shift from a military to a civilian government after the 2019 general election, allowing the Army to adapt to the dynamic digital terrain. The army's adaptation has become more obvious during General Prayut's second term as the Prime Minister, as they have collaborated more frequently with pro-junta political parties.

Before the 2019 election, Palang Pracharath Party (PPRP) was founded in order to enable junta members to retain their government positions after the elections (McCargo and Alexander 2019). The Party then nominated General Prayut as its candidate for the position of Prime Minister in the upcoming election. This demonstrated a solid connection between the PPRP and the military. Moreover, in June 2020, one year after the forming the new coalition government, General Prawit Wongsuwan agreed to step into the role of the new leader of the PPRP. General Prawit, General Prayut, and Gen Anupong Paochinda, collectively known as "the three Ps," exerted control over the country since the 2014 coup and had significant influence over the cabinet (Chambers 2022).

The military, with the support of its coalition political parties, expanded the utilisation of SDIOs. During the motion of no confidence in February 2020, MP Wiroj, from the FFP, explicitly referenced the connection between the military's information operation and a public relations company (Matichon Online 2020), which is co-owned by a member of one of the coalition parties. The PR company recruited approximately 150 employees to engage in posting and commenting on social media platforms, especially Facebook, using fake accounts, to bolster the military-civil government (Interview with informant, November 20, 2023).[2] It is likely that this troll farm functioned in concert with the Army's information operation.

During the 2023 election campaign, suspected SDIOs worked for both government and opposition parties. A journalistic investigation analyzed over

six million Facebook and Twitter messages from a month before and after the election to detect "inorganic" canvassers – accounts showing coordinated activity. It identified five clusters manipulating political opinions: one supporting General Prawit, another promoting the monarchy and government, a third aligned with the MFP, a fourth backing Pheu Thai, and a fifth opposing the government without endorsing a party. While their funding remains unclear, their behavior suggests coordinated inauthentic activity violating social media standards (Amarinthewa 2023), similar to the military-linked accounts banned from 2020 to 2021. Undoubtedly, this raised worries regarding electoral integrity and democratisation in the country (Asia Centre 2023).

Normalising

The RTA had always denied any involvement in SDIOs. For example, in October 2020, when Twitter suspended 926 pro-army accounts, Deputy Army Spokesperson stated that "[t]he issue of IO is a misunderstanding. We don't do this. It's not one of our objectives for using Twitter" (Tanakasempipat 2021). This position had remained unchanged until recently. After the 2023 general election, the military's standpoint has shifted. Instead of declining, the military is attempting to normalise SDIOs.

Following a nine-year period in the cabinet, the popularity of General Prayut, who was the Prime Minister at the time and a prime ministerial candidate for the newly formed United Thai Nation Party, as well as General Prawit, the Deputy Prime Minister and a prime ministerial candidate for the PPRP, has drastically fallen. Nevertheless, both parties remain constituents of the new government under the leadership of Pheu Thai Party as anticipated on the basis of the party's stance during the election campaign. The Pheu Thai Party reversed course and broke its agreement with the FFP, the election winner, and the coalition to establish an anti-junta government (Hicken and Jatusripitak 2023). Subsequently, Sutin Klungsang, an MP from Pheu Thai Party, has been designated as the Minister of Defence, marking the first time a civilian has held this role since the 2014 coup. After two months in the position, he stated:

> Information operations [by the military] are acceptable, but they must be in a positive way. I insist on not undermining anyone or escalating any conflict. However, we must acknowledge that the army is also undermined by IOs. We need to treat the army fairly.
>
> *(Thaipost 2023)*

This interview has two implications. First, it could validate the claims that the Army has engaged in the SDIOs. The Army's IO on social media are

commonly categorised into three wings. The first wing, "black," involves attacking or undermining dissidents. The second wing, "white," aims to legitimise the regime by endorsing the actions of the government, the Army, and the monarchy. The third wing, "grey," provides partisan information in support of the military's agendas (Sombatpoonsiri 2022; Asia Centre 2023). Second, it draws attention to the involvement of other actors, particularly political parties, in conducting comparable IO. The main target of Sutin's assertion is likely to be the FFP, which is believed to have gained large votes from its social media campaigns. The term political "fandom" is employed to explain the party's popularity throughout the election campaign, in which its supporter "*Dom Som*" (ด้อมส้ม)[3] played a significant role (Colombier 2024). Overall, it appears that the Army is attempting to normalise its SDIOs by providing justification for its operations and by claiming that the opposition engages in the same behaviors on its opposition.

Propaganda Model Revisited: A Political Economy of SDIOs

Recent practice of SDIOs demonstrates the dynamic nature of these operations: learning, adapting, and normalising. However, to comprehend the dynamic process of SDIOs, we must understand not only the actors, both state and non-state, but also their interactions with the changing environment, especially communication systems – from mass media to social media. One way to understand SDIOs in a broader context is through a political economy standpoint. The Political Economy of the Media (or Communication) is a branch of the discipline of political economy that focuses on the relations between media and communication systems and the social structure of the society (McChesney 2000), especially "the power relations that mutually constitute the production, distribution and consumption of resources, including communication resources." Political economists mainly analyze how communication is constructed within the society and how it is influenced by the state and businesses (Mosco 2009, 2).

Given that SDIOs involve state and non-state actors manipulating public opinion, analyzing them through the Propaganda Model would provide valuable insights. The Propaganda Model is the core of the Edward S. Herman and Noam Chomsky's seminal book, *Manufacturing Consent*. It is an analytical framework aiming to study the US media and communication system, which emphasises "inequality of wealth and power and its multilevel effects on mass media interests and choices" and argues that "the media serve, and propagandise on behalf of, the powerful societal interests that control and finance them" (Herman and Chomsky 2002, xi, 2). In other words, the Propaganda Model explains the project of "manufacturing consent" or how mass media are designed and operated in order to make people comply with, or consent to "the economic, social, and political agenda of privileged groups

that dominate the domestic society and the state" (Herman and Chomsky 2002, 298). Then, in a manner similar to the making of propaganda, SDIOs are utilised as a stratagem in the political and social flux of the battle about manufacturing consent.

The Five Filters in Social Media Era

Herman and Chomsky's Propaganda Model examines how governments and corporations "filter" the news exposed in order to manipulate people's opinions. The model posits that "[t]he raw material of news must pass through successive filters, leaving only the cleansed residue fit to print" (Herman and Chomsky 2002, 2). This section argues that, in the social media era, the five filters, ownership, advertising, sourcing, flak, and ideology, are different from those in the mass media era. These evolving filters have increased the challenge for both the government and big companies to make people comply with or consent to their agendas. The use of SDIOs demonstrates that both state and non-state actors are struggling to manipulate public opinion in the new communication environments.

Ownership

The Propaganda Model argues that the increasing dominance of a few large corporations in the media business undermines the diversity of opinions and effectively transforms them into a "new private Ministry of Information and Culture" (Herman and Chomsky 2002, 4). There is more concentration of media ownership than when the model was proposed, primarily because of the rise of enormous ICT companies, including social media firms. These social media platforms can effectively prioritise the content that is shown to their users using algorithms (Fuchs 2018; MacLeod 2019).

For a developing country such as Thailand, in contrast to the traditional local mass media producers, the interests of these transnational platforms may not align with those of domestic elites. The removal of accounts associated with the Thai military by Facebook and Twitter serves as a notable instance. Another well-known example of this is a Facebook group called the "Royalists Marketplace," which was set up in April 2020 to serve as a platform for free debate regarding the monarchy (Chachavalpongpun 2020). Once the group reached one million members, Facebook blocked access to the group at the request of the Thai government on the grounds of violating the Computer-Related Crime Act. However, the company stated that "[r]equests like this are severe, contravene international human rights law, and have a chilling effect on people's ability to express themselves" (Tanakasempipat 2020). Within a day, a new group was created, attracting an even larger number of members. There was no further action from the social media platform.

Advertising

Advertising has always been the primary source of revenue for most media outlets. The Propaganda Model suggests that "the private media are major corporations selling a product (readers and audiences) to other businesses (advertisers)" (Herman and Chomsky 2002, 303). However, this old media business model is dissimilar to those of social media. Social media platforms bring about prosumers, who are both producers and consumers of content simultaneously, and use their activities on social media for profit (Fuchs 2021). Then, although advertising has always been the main revenue of media companies, both old media and social media, the product now is their users' data rather than the profiles of users. So, these platforms encourage their users to engage as much as possible so that they may collect more and more data. This has fundamentally changed how news and information are produced and disseminated.

In Thailand, the government and large corporations continue to be the main sources of advertising revenue for the mass media (Achavanuntakul et al. 2024). This has an obvious impact on the news content presented to the audience. However, since the content exposed to social media users is determined by the platforms' algorithm, there is no guarantee that their specific content will be seen and have an influence on people unless they pay these social media companies for targeted advertising.

Sourcing

They also depend more and more on "free content" from the government and corporations. The mass media mainly relies on official sources for content, as they are perceived as "presumptively accurate" (Herman and Chomsky 2002, 19). Additionally, the analysis of the BBC's sourcing shows a growing tendency to rely on the opinions of authorities – mass media increasingly rely on "free content" provided by the government and expert from corporations (MacLeod 2019). However, this may be a lot different on social media since user-generated content is the core feature of social media (Carr and Hayes 2015).

Prior to the social media age, news and information were produced mostly by a few media companies, but social media content creators could be individuals, social media influencers, media outlets, or even political parties and politicians. Thus, people now have various sources of information, and the variety may more and more challenge the project of manufacturing consent. Content shared on social media may originate from official sources, but it also contains comments and opinions that probably go against the authorities' intention. Therefore, this filter may no longer hold the same level of significance as it once did. In Thailand, the younger generation depends on their social media networks as sources of information. Undoubtedly, this poses a threat to the effectiveness of SDIOs.

Flak

Flak is defined as "negative responses to a media statement or program. It may take the form of letters, telegrams, phone calls, petitions, lawsuits, speeches and bills before Congress, and other modes of complaint, threat, and punitive action" (Herman and Chomsky 2002, 26). It may differ depending on the specific time and space settings. In the case of government and businesses, the responses are often prosecutions and lawsuits, including the Computer-Related Crime Act, the Lèse-majesté Provision, and the Defamation Provision. In the case of civic groups, their responses may include boycotts, crowd-funded resistance campaigns.

This filter has been shown to be highly effective and has increasingly been utilised in SDIOs, especially by the authoritarian government. Thailand Lawyers for Human Rights reports at least 1,279 cases related to political participation and expression from youth protests between July 2020 and February 2024. This includes 288 cases charged under the Lèse-majesté Provision and 215 cases charged under the Computer-Related Crime Act (Thai Lawyers for Human Rights 2024). The surge in actions could be interpreted as a reaction from the government, which has lost its grip over the Internet and social media platforms.

Ideology

The Propaganda Model initially introduced anti-communism as an ideological filter. However, with the collapse of the Soviet Union, some scholars suggest replacing the anti-communism filter with non-market mechanisms, anti-terrorism, or anti-Russia (MacLeod 2019). Oddly, in Thailand, the concept of royal nationalism which emerged in the 1970s as an ideological tool used to counter communists continues to be effective to this day. The premise of this ideology is that "a Thai must naturally be a royalist, therefore a non-royalist must not be a Thai" (Winichakul 2014, 80).

The involvement of royalist civic groups, together with organised cyber troops, influences the development of narratives that support the monarchy and has the potential to weaken opposition groups and the democratic political system. They employed patriotic language associated with the monarchy to portray the protesters of 2020 and 2021 as opposing the monarchy and the nation: anti-monarchists and nation-haters. At the same time, pro-regime media outlets depict the demonstrators as vandals supported by Western countries, thereby reinforcing the connection between democracy and disorder, as well as highlighting the involvement of foreign influences in Thailand's sovereignty (Sombatpoonsiri 2022).

Herman and Chomsky acknowledge that the Propaganda Model "describes forces that shape what media does; it does not imply that any propaganda emanating from the media is always effective" (Herman and Chomsky 2002,

xii). In the case of Thailand, the project of manufacturing consent is less effective on the Internet and social media than on the traditional mass media, at least for now. State actors, particularly the Army, and their networks are facing challenges in adapting to the platforms' algorithms and the developing nature of social media users, in terms of maintaining the effectiveness of filters such as ownership, advertising, and sourcing. Instead, they must heavily depend on other filters such as flak and ideology, which is detrimental to the principles of human rights and democracy.

Conclusion

This chapter argues that, to assess the impact of the army's SDIOs, it is crucial to understand the dynamic character of SDIOs. This understanding should encompass not just the actors involved but also their interactions with the dynamic environment, particularly communication technology. State actors, especially the Army, have consistently played a pivotal role in carrying out IO in Thailand. The Thai military's IO, which originated from the counter-communism campaigns in the 1960s, are currently facing challenges in influencing public opinion due to the growth of communication technology like the Internet and social media.

The recent implementation of SDIOs demonstrates the Army's progress in learning, adapting, and normalising its operation. The Army recently acknowledged the significance of social media and subsequently adapted to the social media terrain. They have also enhanced the use of SDIOs to effectively shape public opinion and emotions by collaborating with non-state actors. Currently, with the Pheu Thai Party in control of the government, both the military and the party are making efforts to normalise the IO.

The Propaganda Model has been revisited to illustrate the project of manufacturing consent, which is currently less effective on the Internet and social media compared to traditional mass media. Nevertheless, because state actors and their network possess legal and ideological instruments, the pro-democracy and pro-human rights movements remain at risk, as these tools have the potential to curtail freedom of expression and impede the process of democratisation within the nation.

With Thailand now under civilian government, future research should explore the expanding role of political parties' SDIOs, particularly the supporting functions of their social media political influencers, whether motivated by loyalty or financial incentives – the so-called "Mr and Ms Carrier" (นายแบกและนางแบก) – which appear to exert a measurable influence. Such research would help clarify the ambiguities between state and non-state actors in conducting SDIOs, particularly in hybrid or competitive authoritarian regimes.

Funding: This chapter is part of the project "Cyber Troops and Computational Propaganda in Southeast Asia: A Comparative Study of Public

Opinion Manipulation," funded by the Royal Netherlands Institute of Southeast Asian and Caribbean Studies (KITLV), 2022–2023.

Notes

1 Notably, he was then appointed as the acting director-general of the Public Relations Department (PRD) and eventually became the director-general under General Prayut's government.
2 The interview was conducted in confidentiality and the name of informant is withheld by mutual agreement.
3 In *Thai, som* means orange, the colour associated with the FFP and its successors.

References

Achavanuntakul, Sarinee, Tippatrai Saelawong, Arin Jiajanpong, Phansasiri Kularb, Siwat Uampradit, Ponpakin Phruttiwongwanit, Pattharachai Ornnuam, Khemmapat Trisadikoon, Wichayada Amponkitviwat, and Thunchanok Tangpong. 2024. *Media Organisations' Management of Government and Corporate's Advertising and Public Relations Budget: Towards Crafting Ethical and Transparent Practices*. [In Thai.] Sal Forest (Bangkok). https://salforest.com/knowledge/media-sponsor-transparency.

Amarinthewa, Wongpun. 2023. "'Inorganic' Canvasser: Hunting for 'IO' during the 2023 Election." [In Thai.] *the101.world*, 26 September. https://www.the101.world/unnatural-canvasser-io-election-2023/.

Asia Centre. 2023. *State-Sponsored Online Disinformation: Impact on Electoral Integrity in Thailand*. https://asiacentre.org/wp-content/uploads/State-Sponsored-Online-Disinformation-Impact-on-Electoral-Integrity-in-Thailand.pdf.

BBC Thai. 2020. "IO: The Progressive Movement Reveals Information about the Army Information Operations Network. The Private Sector Issued a Statement Arguing that the Information Was Distorted." [In Thai.] 1 December. https://www.bbc.com/thai/thailand–55145803.

Bradshaw, Samantha, and Philip N. Howard. 2017. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Working Paper no. 2017.12. Project on Computational Propaganda. https://ora.ox.ac.uk/objects/uuid:cef7e8d9–27bf-4ea5–9fd6–855209b3e1f6.

Bradshaw, Samantha, and Philip N. Howard. 2018. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71 (1.5): 23–32.

Carr, Caleb T., and Rebecca A. Hayes. 2015. "Social Media: Defining, Developing, and Divining." *Atlantic Journal of Communication* 23 (1): 46–65. https://doi.org/10.1080/15456870.2015.972282.

Chachavalpongpun, Pavin. 2020. "Constitutionalizing the Monarchy: Uncompromising Demands of Thai Protesters." *Journal of International Affairs* 73 (2): 163–172.

Chambers, Paul. 2022. "Thailand in 2021 Angling towards Chaos?" In *Southeast Asian Affairs 2022*, edited by Daljit Singh and Thi Ha Hoang, 343–361. Singapore: ISEAS–Yusof Ishak Institute Singapore.

Colombier, Alexandra. 2024. *How Thailand's Move Forward Party's Fandom Strategy Shaped the 2023 General Election*. Singapore: ISEAS–Yusof Ishak Institute.

Fuchs, Christian. 2018. "Propaganda 2.0: Herman and Chomsky's Propaganda Model in the Age of the Internet, Big Data and Social Media." In *The Propaganda Model Today: Filtering Perception and Awareness*, edited by Joan Pedro-Carañana, Daniel Broudy, and Jeffery Klaehn. London: University of Westminster Press.

Fuchs, Christian. 2021. *Social Media: A Critical Introduction*. Third ed. London: SAGE.

Giglietto, Fabio. 2022. Coordinated Inauthentic Behavior. In *Elgar Encyclopedia of Technology and Politics*, edited by Andrea Ceron. Cheltenham, UK: Edward Elgar Publishing.

Goldstein, Josh A., Aim Sinpeng, Daniel Bush, Ross Ewald, Jennifer John, and David Thiel. 2020. *Cheerleading without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army*. https://cyber.fsi.stanford.edu/publication/cheerleading-without-fans-low-impact-domestic-information-operation-royal-thai-army.

Herman, Edward S., and Noam Chomsky. 2002. *Manufacturing Consent: The Political Economy of the Mass Media*. Second ed. New York: Random House.

Hicken, Allen, and Napon Jatusripitak. 2023. "Introduction: Making Sense of Thailand's Seismic Elections." *Contemporary Southeast Asia* 45 (3): 335. https://doi.org/10.1355/cs45-3a.

Johnson, Kay, Panu Wongcha-um, and Panarat Thepgumpanat. 2019. "'The Threat Now is Fake News': Thai Army Chief Describes 'Hybrid War'." *Reuters*, 10 August. https://www.reuters.com/article/idUSKCN1UZ1L3/.

Kemp, Simon. 2020. "Digital 2020: Thailand." *Global Digital Reports*. https://datareportal.com/reports/digital-2020-thailand.

Lertchoosakul, Kanokrat. 2021. "The White Ribbon Movement: High School Students in the 2020 Thai Youth Protests." *Critical Asian Studies* 53 (2): 206–218. https://doi.org/10.1080/14672715.2021.1883452.

MacLeod, Alan. 2019. *Propaganda in the Information Age: Still Manufacturing Consent*. London: Routledge.

Matichon Online. 2020. "'Wiroj' Reveals 4 Main Missions of 'IO' Operation 'Big Tu' Divides the People – Inherits Power." [In Thai.] 27 February. https://www.matichon.co.th/politics/news_2007395.

McCargo, Duncan. 2017. "New Media, New Partisanship: Divided Virtual Politics In and Beyond Thailand." *International Journal of Communication*, 4138.

McCargo, Duncan, and Saowanee T. Alexander. 2019. "Thailand's 2019 Elections: A State of Democratic Dictatorship?" *Asia Policy* 14 (4): 89–106. https://doi.org/10.1353/asp.2019.0050.

McChesney, Robert W. 2000. "The Political Economy of Communication and the Future of the Field." *Media, Culture & Society* 22 (1): 109–116. https://doi.org/10.1177/016344300022001006.

Mosco, Vincent. 2009. *The Political Economy of Communication*. Second ed. London: SAGE Publications.

National Defence Studies Institute. 2016. *Strategic Communication and Information Operations of the Royal Thai Army: Guidelines for Future Operations*. [In Thai.] National Defence Studies Institute (Bangkok). https://www.sscthailand.org/uploads_ssc/research_20180823153500669963601l.pdf.

News Agencies and Post Reporters. 2020. "Twitter Takes Down Thai Army IO Network." *Bangkok Post*, 9 October. https://www.bangkokpost.com/thailand/general/1999463/twitter-takes-down-thai-army-io-network.

Prachatai. 2011. "CRES Spokesperson Admits to Composing 'Anti-Monarchy Plot Diagram' in Response to Defamation of Lady Charungjit." [In Thai.] 26 May. https://prachatai.com/journal/2011/05/34974.

Ruijgrok, Kris, and Yatun Sastramidjaja. 2023. *Cyber Troops and Computational Propaganda in Southeast Asia: A Comparative Study of Public Opinion Manipulation*. Paper presented at the ECPR General Conference, Panel on Digital Authoritarianism and Regime Change. European Consortium for Political Research. https://ecpr.eu/Events/Event/PaperDetails/68961

Scott-Railton, John, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, and Ron Deibert. 2022. "Pegasus Spyware Used Against

Thailand's Pro-Democracy Movement." 17 July. https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/.
Sinpeng, Aim. 2021. "Hashtag Activism: Social Media and the #FreeYouth Protests in Thailand." *Critical Asian studies* 53 (2): 192–205. https://doi.org/10.1080/14672715.2021.1882866.
Sinpeng, Aim. 2024. "Social Media and the DIY Politics in Thailand's 2023 Election." *Pacific Affairs* 97 (1): 99–116. https://doi.org/10.5509/2024971-art5.
Sombatpoonsiri, Janjira. 2022. "'We Are Independent Trolls': The Efficacy of Royalist Digital Activism in Thailand." *ISEAS Perspective* 2022/1. https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-1-we-are-independent-trolls-the-efficacy-of-royalist-digital-activism-in-thailand-by-janjira-sombatpoonsiri/.
Sombatpoonsiri, Janjira, S. Tyler Williams, Wongpun Amarinthewa, and Suppalerk Petchpo. 2023. *Unmasking Digital Harassment in Thailand: A Study of Online Smear Campaigns and the Impact on Civil Society*. Institute of Asian Studies Monitoring Centre on Organised Violence Events (MOVE), Chulalongkorn University. https://www.the101.world/wp-content/uploads/2023/11/Unmasking-Digital-harassment-in-Thailand_FINAL–1.pdf.
Tanakasempipat, Patpicha. 2020. "After Block, New Facebook Group Criticising Thai King Gains 500,000 Members." *Reuters*, 25 August.
Tanakasempipat, Patpicha. 2021. "Facebook Removes Thai Military-linked Information Influencing Accounts." *Reuters*, 4 March. https://www.reuters.com/article/idUSKCN2AV277/.
Thai Lawyers for Human Rights. 2020. "Joint Statement: State-backed Online Information Operation Against Human Rights Defenders Must Be Fully Investigated and Immediately Halted." 2 March. https://tlhr2014.com/en/archives/16303.
Thai Lawyers for Human Rights. 2024. *February 2024: 1,279 Political Lawsuits Were Filed Against 1,951 People*. https://tlhr2014.com/en/archives/65625.
Thaipost. 2023. "'Sutin' Gives Green Light to the Army to Create Creative 'IO' Don't Destroy Each Other Like the Opposition." [In Thai.] 31 October. https://www.thaipost.net/x-cite-news/476599/.
Thammasat University Research and Consultancy. 2020. *Survey of Consumer Behavior and Trends on Media Consumption in Thailand*. [In Thai.] Office of the National Broadcasting and Telecommunication Commission (Bangkok).
Today. 2020. "ISOC Admit Allocating the Budget to pulony.blogspot.com." [In Thai.] 27 February. https://workpointtoday.com/pulony-military-confirm/.
Winichakul, Thongchai. 2014. "The Monarchy and Anti-Monarchy: Two Elephants in the Room of Thai Politics and the State of Denial." In *Good Coup Gone Bad: Thailand's Political Development since Thaksin's Downfall*, edited by Pavin Chachavalpongpun, 79–108. Singapore: ISEAS–Yusof Ishak Institute Singapore.

7

TURKISH GOVERNMENT'S DOMESTIC DIGITAL INFORMATION OPERATIONS ON X (TWITTER), DEMOCRACY, AND SOCIAL COHESION

Ihsan Yilmaz, Bulent Kenes, and Nicholas Morieson

Introduction

In recent years, the digital sphere has evolved into a central arena for political contestation and control. In authoritarian and hybrid regimes, the digital ecosystem is no longer merely a site of grassroots activism or political communication but has become a space strategically weaponised by ruling elites to manipulate public opinion, suppress dissent, and consolidate power. This chapter explores the mechanisms and implications of such manipulation in Turkey, focusing on the digital strategies employed by the ruling Justice and Development Party (AKP) under the leadership of President Recep Tayyip Erdoğan. It situates Turkey as a paradigmatic case of how SDIOs are used by authoritarian populist regimes to dominate the information space and reshape the emotional and cognitive frames through which citizens perceive politics and society.

Turkey's drift into digital authoritarianism has been accompanied by a broader restructuring of its media and communication environment. With a severely weakened free press and the near-total capture of mainstream media, the Erdoğan regime has turned the internet – and especially social media – into a tool for amplifying state narratives and silencing alternative voices. Through a combination of regulatory pressure, economic coercion, legal harassment, and targeted repression, the regime has forced independent media owners out, installed partisan allies in key media institutions, and silenced dissenting journalists. Building on this control of traditional media, the government has expanded its influence into the digital realm through coordinated and multilayered online operations that exemplify the key

DOI: 10.4324/9781003628088-10
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

features of SDIOs: emotional mobilisation, disinformation, identity-based polarisation, and transnational outreach.

This chapter begins by examining the role of AK trolls, state-aligned digital actors often presented as grassroots supporters, who play a crucial role in shaping online discourse. These actors engage in targeted harassment, amplify regime-friendly narratives, and attack opposition voices, thus manufacturing consent and suppressing counter-narratives in Turkey's online spaces. It then turns to the use of automated bots, which systematically disseminate political propaganda, manipulate trending topics, and create the illusion of widespread support or opposition. These bots are instrumental in overwhelming critical voices and shaping the digital public sphere in favor of the regime.

The chapter also investigates the activities of hackers, whose cyber intrusions target opposition groups, journalists, and activists. These operations serve to intimidate, extract compromising information, and reinforce the perception that dissent is not only dangerous but futile. Together, trolls, bots, and hackers constitute a digital vanguard that enforces ideological conformity and expands the reach of Erdoğan's regime.

A final key component of Turkey's SDIOs is the strategic use of emotive political communication on social media. The regime constructs emotionally charged narratives around the idea of a "New Turkey," reinforcing Erdoğan's personality cult as the embodiment of national strength, piety, and destiny. The AKP's civilisational populist "New Turkey" narrative

> has a strong emphasis on a fully independent, very strong Turkey that is a leading regional and even global power. One of the most note-worthy features of the mission is that it is presented as a "native" and "national" strategy. Accordingly, since he seized absolute power, Erdoğan has presented himself as the chief (in Turkish reis), the wise, native and national (*yerli and milli*) leader of the Turkish people who executes the mission.
>
> *(Yilmaz et al. 2020, 272)*

The concept of the New Turkey is grounded in three core ideas: independence, democracy, and development. Independence refers to breaking free from Western influence, a view that resonates strongly with nationalist and conservative segments of Turkish society. This sentiment also reflects Turkey's long-standing insecurity in its relationship with the West. Democracy, in this vision, is based on a majoritarian model led by a powerful figure who embodies the national will, supported by compliant institutions. This approach mirrors other forms of centralised governance seen in similar contexts. Development, meanwhile, is framed as achieving economic, military, and political strength to position Turkey as a global power. Assertive foreign policy actions, particularly in Syria and Iraq, are presented as evidence of this new stature. This vision appeals across ideological lines – from secular

and religious nationalists to Kemalists and Eurasianists. While some secular elites are uneasy with the revivalist Ottoman tone, Erdoğan carefully adjusts his rhetoric, invoking the legacy of Atatürk to temper concerns and build broader legitimacy. The overarching message – a strong, independent Turkey free from internal and external enemies – finds broad appeal. The ideational narrative driving this vision draws on nationalism, tradition, religion, and identity. It promotes the idea of restoring Turkey's historical greatness as a leading Muslim nation. The failed coup of 2016 became a turning point, allowing Erdoğan to frame dissenters as internal enemies manipulated by foreign powers. Foreign policy has served to legitimise the regime's authoritarian turn, reinforcing narratives of national strength and global relevance (Yilmaz et al. 2020, 272).

These narratives often portray opposition actors as internal enemies or existential threats, legitimising repression under the guise of national unity and security. The demonisation and criminalisation of Gezi Park protesters serves as a powerful case study of this tactic, where state-controlled narratives framed dissenters as traitors, terrorists, or foreign agents. Through such discursive practices, the government fosters a culture of fear, division, and loyalty that not only inhibits opposition but also secures emotional allegiance from its support base.

By dissecting these strategies, the chapter contributes to a broader understanding of how digital technologies are repurposed by authoritarian regimes to operationalise SDIOs. Turkey offers a compelling case of how state-led digital campaigns fuse emotional resonance with computational efficiency to control narratives, mobilise affect, and entrench authoritarian governance in the digital age.

Organising Grassroots Campaigns for Online Manipulation

In line with the global trend among authoritarian regimes, the Erdoğan administration has leveraged cyber-enabled IO to shape political discourse, distort public perception, and conceal allegations of misconduct, corruption, and human rights violations (Fixler 2023). One of the regime's most effective strategies involves constructing the illusion of widespread grassroots support through coordinated digital campaigns. These are particularly active during politically sensitive periods such as elections, when the regime's need to dominate the narrative intensifies.

A central tactic involves the deployment of extensive networks of fake, compromised, or anonymous accounts designed to amplify pro-government messaging. These networks, composed of a mix of trolls, bots, and astroturfers, are used to create the impression of popular endorsement of AKP policies and leadership (HRW 2023). Within the Turkish-speaking Twitter community, such actors wield significant influence over the circulation of

information, operating as part of highly interconnected retweet rings and influencer-troll alliances. Together, these accounts disseminate propaganda, disinformation, and emotionally charged narratives, forming a core component of Turkey's SDIOs.

AK Trolls

The systematic deployment of AK Trolls represents a key pillar in the Erdoğan regime's digital strategy. Social media platforms – particularly X (formerly Twitter), which boasts over 16 million users in Turkey (Minto 2023) – serve as primary arenas for these operations. The regime's use of trolls dates back to the Gezi Park protests of 2013, when widespread media censorship led citizens to turn to Twitter for uncensored news and open political debate (Yılmaz and Turner 2019). In response, the AKP initiated a formalised campaign, reportedly recruiting and training around 6,000 young party members to disseminate pro-government content (Albayrak and Parkinson 2013). These troll networks are not ad hoc; they are strategically planned, coordinated, and resourced.

Trolls frequently operate using sock puppet identities – accounts that simulate diverse ideological affiliations (e.g., Kemalist, Kurdish, or nationalist) – to infiltrate opposition conversations and manipulate discourse from within. This technique of political astroturfing enables the regime to covertly shape public narratives and discredit dissenting voices under the guise of authentic engagement. The AKP's digital army, reportedly comprising over 2.1 million active users, engages in a wide range of activities: defending Erdoğan, vilifying political opponents, harassing journalists, disseminating fabricated content, and even conducting cyber surveillance (Daily Motion 2020; Akca et al. 2021).

The AK Trolls are not merely autonomous actors but operate with significant institutional and financial support from the regime and affiliated businesses. Backed by intelligence services, they often enjoy impunity, operating beyond the reach of legal accountability (Akca et al. 2021). In their earlier iterations, troll activity relied heavily on automated bots generating repetitive hashtags in support of Erdoğan. Over time, their sophistication evolved into "retweet rings," wherein members form coordinated clusters that mutually amplify content. These networks, with names like "AK Davam Retweet Groups 1&2," artificially inflate hashtag popularity and distort trending topics (Akis 2022).

AKP-affiliated trolls use diverse tactics to dominate the digital space. These include orchestrated hashtag campaigns, the systematic harassment of opposition figures, and mass reporting of accounts to prompt suspensions. Government officials have openly celebrated these activities. For instance, the Head of the Ottoman Hearths in Eskişehir, proclaimed: "We command a social

media army of 200,000 people . . . fighting for the 2023 goals, swearing to elevate Erdoğan to a leadership role within the ummah" (Ablak 2022). Trolls have also played a central role in targeted online harassment campaigns. When Erdoğan challenged the public to say "enough" if they wanted him to step aside, the hashtag #TAMAM quickly went viral. In retaliation, the troll networks pushed the counter-hashtag #DEVAM ("onwards"), underscoring the regime's agility in neutralising digital dissent (Akis 2022).

Journalists have been frequent targets of these attacks, especially after being singled out by government officials. Trolls reply en masse to critical tweets with defamatory allegations, coordinate reporting campaigns, and circulate smear narratives to damage reputations and trigger legal consequences. In several cases, this online harassment has preceded the arrest or detention of the targeted individuals (Akis 2022).

Beyond individual accounts, the regime also operates through proxy organisations that appear to be independent civil society groups. These organisations, often espousing Islamist or ultranationalist ideologies, help promote regime narratives. One notable example is the IHH Humanitarian Relief Foundation, a pro-government charity with radical leanings, which promoted the hashtag #GazzeAblukaAltinda ("Gaza Under Siege") in alignment with Erdoğan's foreign policy positioning on Palestine (Topcu 2020).

Bots

Automated bots represent a central component of SDIOs, particularly in authoritarian contexts where controlling digital discourse is critical to regime stability. In Turkey, bots are deployed at scale to simulate grassroots support, manipulate social media algorithms, and promote regime-approved narratives. As with other countries like Brazil and the US, Turkey has faced extensive bot-driven manipulation, but it stands out for having one of the highest bot infection rates globally, as highlighted by the Media Literacy Index (Lessenski 2023).

Unlike conventional social media users, these bots rarely engage in sustained dialogue. Instead, they focus on promoting fake trends by exploiting vulnerabilities in platform algorithms. Elmas (2023) notes that nearly 20% of active Twitter users in Turkey encounter bot behavior, as these bots imitate human activity through automated actions. The Erdogan regime and its supporters use these bots to amplify propaganda, counter anti-government messaging, and engineer the illusion of popular consensus – an astroturfing strategy designed to drown out dissenting voices (Karatas and Saka 2017).

Between 2015 and 2022, over 212,000 bots were responsible for generating more than 29,000 fake trends, constituting up to 52% of daily trending topics (Elmas 2023). The prevalence of such manipulation varied over time.

In early 2021, fake trends accounted for 30% of daily activity. After bot purges by Twitter in late 2021, the figure dropped to 10% by March 2022, only to rise again to 20% by November 2022. During the 2023 Turkish elections, the fake trend percentage fluctuated between 9% and 35%, with spikes observed on politically strategic days. Notably, 87% of bot accounts remained silent for at least one month, a tactic that hinders bot-detection systems (Elmas 2023).

In May 2023, Turkey recorded 145 million tweets from 12.5 million accounts, with 23% identified as bots by the Turkish General Directorate of Security. Analysis of the top ten trending hashtags revealed that 52% of the accounts using them were bots (Bulur 2022). Further reports noted the reactivation of over 12,000 Russian- and Hungarian-speaking Twitter accounts, alongside Turkish-speaking bots, with the intent of artificially boosting engagement and visibility.

Despite Twitter's relatively modest penetration in Turkey – estimated at 27% of the population – the platform wields disproportionate influence over political discourse. Between 2013 and 2023, up to half of trending topics on Turkish Twitter were manipulated by bots (Unker 2023). These efforts illustrate how SDIOs leverage automation to generate attention, distract from inconvenient narratives, and polarise the digital public sphere in favor of authoritarian incumbents.

Hackers

Another crucial pillar of Turkey's digital authoritarianism is the use of hackers to target domestic and international opponents. While initially framed as part of Turkey's cyber-defense strategy, hacking has become integral to broader SDIO tactics, with state-linked or ideologically aligned groups conducting cyber intrusions to silence critics, intimidate opposition, and project nationalist messages abroad (Yesil et al. 2017).

As early as 2009, Erdogan-aligned hackers began targeting foreign critics. A hacker defaced Dutch politician Geert Wilders' website, replacing his image with that of a monkey (Souli 2018). Domestically, independent media institutions such as the Cihan News Agency, Taraf, Zaman, and Cumhuriyet were victims of major cyberattacks during critical elections in 2014 and 2015, raising concerns about the state's involvement or complicity.

Hacktivist groups like Aslan Neferler Tim (ANT) and Ayyildiz Tim have conducted coordinated cyber operations against targets in Europe, North America, and the Middle East. ANT was implicated in cyberattacks on Austrian institutions in 2016 (Souli 2018), while Ayyildiz Tim took control of numerous high-profile Twitter accounts – including those of Forbes, Amnesty International, and BBC North America – in 2017 to disseminate pro-Erdogan propaganda. These messages included hashtags such as #NaziGermany and

#OttomanSlap and redirected users to pro-government content on YouTube (Hern 2017).

Hackers operating in Turkey have also targeted government critics directly. In one instance, a cybersecurity consultant illegally accessed a critic's account and informed Erdoğan's office – only for the regime to investigate the victim rather than the hacker (Bozkurt 2022). During heightened tensions between Turkey and the US in 2018, Ayyildiz Tim allegedly hacked the social media accounts of prominent American journalists to post Erdogan-supportive content, with evidence of potential links to Turkish security forces (Goud 2018).

The Erdogan regime's support for hacking culture is visible in its institutionalisation of cyber activities. Events like "Hack Istanbul," launched in 2018, bring together global hackers to simulate real-world attack scenarios. These competitions, backed by the Turkish Presidency's Digital Transformation Office, offer financial rewards and national recognition (Hurriyet Daily News 2021). Similarly, the Cyber Intelligence Contest has expanded training in offensive cyber operations, reflecting the regime's ambition to scale up its SDIO capabilities (Cyber Intelligence Contest 2021).

The use of hacking as an extension of SDIO strategy has also been directed toward foreign relations. In January 2023, the Turkish group Türk Hack Team launched cyberattacks on Swedish government websites in retaliation for Quran desecration incidents. Declaring themselves nationalist but unaffiliated with the state, the group threatened to leak sensitive personal data of Swedish citizens (Hull 2023). Meanwhile, opposition leaders in Turkey – most notably Kemal Kılıçdaroğlu – accused the ruling party of hiring foreign hackers to produce deepfakes and spread disinformation during the 2023 elections.

These activities underline the Erdogan regime's reliance on cyber operations not only as instruments of domestic control but as tools of international projection. By enabling and supporting hacking initiatives through both official and unofficial channels, the regime has extended its influence far beyond national borders, using digital coercion as part of a broader authoritarian strategy. Within the SDIO framework, hacking functions as both a tactical and symbolic operation: disrupting democratic infrastructures, intimidating opposition, and asserting nationalist dominance in a digitised information order.

Emotive Political Mobilisation on Social Media

SDIOs often merge historical grievances with religious symbolism to enhance narrative credibility and emotional impact. States use nationalist myths – fabricated accounts aimed at building unity and portraying the nation in a favorable light (Yilmaz et al. 2023a). Authoritarian regimes, in particular,

utilise digital platforms to construct narratives that resonate with specific societal groups, often by evoking victimhood to stir emotions (Yilmaz 2021). In Turkey, the Erdogan regime has strategically embedded Islamic motifs and revised Ottoman history into its messaging to strengthen influence over the public (Yilmaz 2021; Yilmaz et al. 2023b). Within such a polarised media landscape, competing versions of reality circulate, making it increasingly difficult for citizens to discern truth from falsehood (Humprecht et al. 2020). This context of polarisation, disinformation, and populism is underpinned by shared psychological dynamics (Marwick and Lewis 2017; Humprecht et al. 2020).

Erdogan's regime employs a three-part rhetorical structure to provoke emotional engagement: a nostalgic glorification of a pure and united past, a present in crisis blamed on external interference or trauma, and a promised utopian future attainable through national solidarity. These elements are structured around binary contrasts that position the past and future in opposition to a troubled present (Levinger and Lytle 2001). Victimhood narratives – often supported by conspiracy theories and partial truths – serve to legitimise the regime and suppress opposition (Yilmaz and Shipoli 2022). Erdogan's own narrative of persecution dates back to his imprisonment in 1999 but has been increasingly invoked during political crises such as the 2013 Gezi Park protests, the corruption scandal that same year (Lancaster 2014), and the failed coup attempt in 2016. Against the backdrop of internal strife and external alienation, Erdogan is framed as the sole guardian of national identity and sovereignty (Gulseven 2021; Turk 2018).

New Turkey, Rising Turkey, and Turkish Century

Narratives like "#NewTurkey," "#RisingTurkey," and "#TurkishCentury" function as both symbolic and strategic tools in Erdogan's communication arsenal. These narratives, laden with ideological, cultural, and political meaning, aim to delegitimise the secular, Western-oriented establishment of the "Old Turkey." Introduced in 2013, the "New Turkey" discourse has justified a series of polarising decisions – from the construction of a lavish presidential palace and the adoption of a presidential system in 2017, to military operations in Syria. While initially inclusive, the narrative has become increasingly divisive and authoritarian, drawing criticism domestically and internationally as indicative of democratic backsliding.

In parallel, the regime has escalated social media operations, with troll networks promoting hashtags like "#YouWillNotSucceed" and "#CountDownForBigTurkey" to counteract growing unrest related to economic decline and social discontent. During periods of currency devaluation, these accounts downplayed the crisis, instead calling for national unity to defend sovereignty.

This propaganda also reflects the regime's nativist turn, which emphasises nationalism, Islamism, anti-elitism, protectionism, and xenophobia. It frames the regime as the sole representative of the "national will" (#MilliİRade), branding all dissenters as traitors or agents of foreign powers (Kiniklioglu 2017; Turk 2018).

Nativism, Local and National

Since 2015, the Erdogan regime has increasingly emphasised themes of nativism and nationalism, promoting projects under the banner of "#YerliveMilli" ("local and national"). This discourse gained traction following the July 15, 2016, coup attempt, with the Gülen movement labeled as a terrorist organisation and growing anti-Western sentiment fueling nationalist populism. Erdogan's alignment with ultranationalist factions allowed him to frame himself as the nation's savior, blending religious conservative grievances with nationalist isolationism (Gulseven 2021). The "local and national" rhetoric has since been used to justify diverse policies, from domestically produced automobiles to the purchase of Russian S-400 missile systems and development of indigenous digital infrastructure.

Erdogan also seeks to reframe Turkish identity by replacing the secular, pro-European Kemalist legacy with a neo-Ottoman, Islamic, and conservative vision. This includes the downgrading of republican holidays and civil milestones, such as the muted celebrations of the Republic's centenary, justified by international events like the Israel-Gaza conflict. In speeches, such as one in Istanbul in March 2017, Erdogan presents Islam and Turkish tradition as the true civilisation in opposition to the West, advocating for re-Islamisation and re-nationalisation.

Erdogan's Personality Cult

A defining element of Erdogan's enduring appeal is the personality cult that surrounds him. AKP officials have attributed exaggerated qualities to him, referring to Erdogan as the "eternal president," a "caliph," or even implying divine attributes (Lancaster 2014).

This image has been reinforced through an expansive social media strategy in multiple languages. Hashtags like #WeAreErdogan, #ErdoganIsTheLeaderOfTheWorld, #BraveHeartErdogan, #ölümüneerdoğan (#UntilDeathWithErdogan), and others receive massive engagement. Some even include authoritarian demands such as "#idamistiyoruzsesimiziduyr eceptayyiperdoğan" (we want capital punishment, hear us Recep Tayyip Erdogan). During the 2017 constitutional referendum, hashtags like #TurkeySaysYes and #YeniAnayasaGüçlüTürkiye were also widely used (Grossman et al. 2020).

These hashtags trend globally, aided by troll and bot activity as well as high-profile endorsements, such as that of actress Lindsay Lohan – allegedly paid by the regime (The Express Tribune 2016). While most usage is in Turkish (72.73%), the messages also gain traction in English (9.09%), Indonesian (6.06%), and other languages, demonstrating the regime's ambition to project Erdogan's image beyond Turkey's borders.

Targeting Opposition as Internal Enemies

The Erdogan regime promotes a nativist, conservative, and religiously infused political stance, positioning Sunni Islam as central to Turkish identity. This aggrieved nativism often results in xenophobia and racism, adversely affecting ethnic, religious, and political minorities such as Kurds, Alevis, Gülenists, and Syrian refugees (Kiniklioglu 2017).

During the 2013 Gezi Park protests, the internet and social media played crucial roles in enabling horizontal communication, activism, and political participation, particularly amid a domestic media blackout (Burke and Sen 2018). In response, Erdogan condemned social media platforms, infamously calling Twitter a "menace" (Hutchinson 2013). Rather than addressing the protests' root causes, he attributed the unrest to vague "outside forces" and constructed imaginary enemies, such as the "interest-rate lobby" (Idiz 2013). Pro-government media circulated conspiracy theories, portraying the protests as externally orchestrated. Erdogan labeled demonstrators as marauders (çapulcu) and accused internal traitors and foreign collaborators of coordinating the events (Hurriyet Daily News 2023).

Some pro-government outlets went further. Yeni Safak claimed the protests were engineered by Otpor!, a Serbian civil society group, while Deputy PM Besir Atalay blamed foreign agents and the Jewish diaspora. Turkish officials and commentators floated accusations involving Jewish groups, Mossad, and Germany (Nefes 2017). This marked the beginning of the Erdogan regime's systematic efforts to control digital narratives using troll networks (Akis 2022). In the lead-up to the 2014 presidential elections, AK Trolls framed the Gezi protests as a coup attempt, linking them with Egypt's 2013 military coup through hashtags like #ArrestTaksimCoupPlatformMembers and #NoToCoupInEgypt. This campaign eventually led to extensive criminalisation, culminating in the life sentence of businessman and human rights activist Osman Kavala (Poole 2022).

Throughout the Gezi protests, Erdogan portrayed the opposition Republican People's Party (CHP) as internal enemies. He alleged that most protesters were CHP voters and accused party leader Kilicdaroglu of acting like a terrorist leader (Hurriyet Daily News 2013). In 2014, AK Trolls promoted hashtags like #TurkeyIsBetterWithErdogan and #ShameForTurkeyCHP to contrast Erdogan's development agenda with CHP's alleged legacy of chaos.

Leading up to the 2015 elections, hashtags such as #ŞeddeliFaşistCHP and #CHPyeRağmenDireniyoruz intensified anti-CHP narratives (Grossman et al. 2020). Erdogan's inflammatory language further escalated tensions. In April 2016, he asked, "What are we going to do about political perverts?" referring to Kilicdaroglu, triggering the viral hashtag #SiyasiSapıkKılıçdaroğlu (Gazeteport 2016).

Following the 2016 coup attempt, the regime's digital campaigns depicted the CHP as sympathetic to the coup plot. Hashtags like #Taksimdeyiz implied that CHP members would have celebrated a successful coup. These narratives also endorsed violence, evidenced by an AKP supporter physically assaulting Kilicdaroglu at a soldier's funeral in 2019.

In the 2019 local elections, AK Trolls launched a coordinated smear campaign. Hashtags such as #CHPİPinPKKlıadayları and #CHPPKKnınİzinde aimed to associate the CHP with the outlawed PKK (Elmas et al. 2019). Semantically neutral hashtags like #CHPdeKriz were strategically used to sow division within the party. Ekrem Imamoglu, the CHP candidate for Istanbul mayor, was targeted with hashtags like #EkrandakiYalancı, #HırsızVar, and #ÇünküÇaldılar. He was falsely portrayed as the front for a conspiratorial alliance involving the Gülen movement, Zionists, and the PKK.

In 2022, Kilicdaroglu disclosed a comprehensive troll investigation, revealing a treasury-funded network of 10,000–12,000 troll accounts organised in a hierarchical structure, each disseminating thousands of posts (Ablak 2022).

Digital Manipulation During the 2023 Elections

The 2023 elections were marred by digital manipulation and media asymmetry. Erdogan dominated television coverage, appearing on 18 channels just two days before the election, while Kilicdaroglu received limited airtime and relied primarily on social media (Selcuki 2023). Erdogan's supporters pushed slogans such as #BaşkaLiderMiVar and #YaparsaErdoganYapar to reinforce his cult of personality.

Erdogan's campaign framed the opposition as agents of chaos and terror. He weaponised Kilicdaroglu's Alevi background and used anti-LGBTQ+ rhetoric to portray the opposition as a threat to national values. Interior Minister Soylu called the election a "coup attempt" (Korkmaz 2023). Erdogan also linked the opposition to the PKK, citing HDP support for Kilicdaroglu as evidence. A manipulated video showing PKK leader Murat Karayilan appeared at an Erdogan rally, an unprecedented tactic even acknowledged by Erdogan (Selcuki 2023). Fake election brochures resembling Kilicdaroglu's materials were circulated to mislead voters.

The regime's digital misinformation machinery also targeted symbolic issues. A photo of Kilicdaroglu standing on a prayer rug with shoes on was

used to stir religious outrage, spreading rapidly via the hashtag #seccade (Unker 2023). Another campaign misrepresented a statement on "municipal autonomy" by CHP deputy Yunus Emre, using the hashtag #ozerklik to trigger fears of national disintegration (Unker 2023).

Extending Repression to Kurds and the HDP

The HDP, particularly co-chair Selahattin Demirtas, opposed Erdogan's proposed presidential system. In response, the regime hardened its anti-Kurdish stance, especially during and after the 2014 Kobane crisis (Marschall and Konak-Unal 2021). Erdogan's party began courting nationalist voters by claiming that Turkey did not have a Kurdish issue but a terrorism problem (Karakaya-Polat 2018).

The state of emergency declared after the 2016 coup attempt enabled extensive crackdowns. Nineteen HDP MPs, including co-chairs, were arrested, and thousands of party members were detained (Tahiroglu 2021). The government replaced HDP mayors with AKP-appointed trustees in dozens of municipalities, denying elected officials their mandates (Marschall and Konak-Unal 2021).

In 2019, during "Operation Peace Spring," the regime launched a digital campaign to reframe its military actions in Syria as counterterrorism. Hashtags like #TurkeyJustKilledTerrorists and #TurkeyFightsISISandYPG were used to promote a sanitised narrative, even as bot-like accounts amplified #BabyKillerPKK (Grossman et al. 2020).

Narratives Against the Gülen Movement

During the December 2013 corruption scandal, the Erdogan regime used digital campaigns to deflect blame and demonise the Gülen movement. Trolls employed hashtags such as #MontajÇetesiİhanetŞebekesi and #CorruptionIsPretextTreasonIsReal to delegitimise the corruption allegations. The narrative framed the investigations as a CIA-backed "judicial coup."

After the 2016 coup attempt, pro-Erdogan accounts launched a barrage of hashtags like #TerroristGulen and #gameoverUSA (Yildiz and Smets 2019), promoting the regime's version of events. These campaigns incited widespread hatred, dehumanisation, and calls for capital punishment.

According to the Stockholm Center for Freedom, Erdogan has used over 240 derogatory terms to describe the Gülen movement, including "blood-sucking leeches," "cancer cells," and "traitors" (Kenes 2020, 79). This rhetoric, amplified across social and traditional media, has been instrumental in shaping public opinion. The regime labeled the movement as FETO, which has generated over 178 million Google results as of October 2023 (Kenes 2020, 80).

Conclusion

In democratic contexts, the rapid dissemination of disinformation, misinformation, and divisive narratives poses a profound threat to social cohesion and institutional legitimacy. SDIOs, by exploiting the affordances of digital platforms, aim to inflame polarisation and deepen existing social, political, and ideological fractures. In doing so, they undermine trust – arguably the cornerstone of functioning democracies – and render public discourse increasingly vulnerable to manipulation. As demonstrated in the case of Turkey, the erosion of trust has repercussions that extend far beyond individual beliefs, corroding the credibility of democratic institutions and processes.

SDIOs are engineered to provoke a range of emotional responses – negative, positive, and ambivalent – depending on their intended effect. This emotional manipulation serves multiple strategic goals: consolidating support for authoritarian leaders, delegitimising political opponents, discrediting independent media, and destabilising civil society. These engineered affective responses – such as fear, resentment, and anger – do not remain confined to the digital sphere. They permeate the broader social fabric, contributing to intergroup hostility, xenophobia, and civic disengagement, which in turn can catalyze dissent and unrest.

The Turkish context offers a compelling case study of how SDIOs are operationalised within an authoritarian populist framework. Through coordinated digital campaigns utilising AK trolls, bots, and state-aligned hackers, the regime has effectively turned the digital space into a battlefield of ideological dominance. The construction of emotive and polarising narratives – such as the mythologising of a "New Turkey," the elevation of Erdogan through a cultivated personality cult, and the strategic vilification of the opposition as internal "others" – demonstrates how digital propaganda can shape political imaginaries and consolidate power.

Equally alarming is the regime's use of SDIOs to criminalise dissent, delegitimise opposition parties, and suppress alternative viewpoints. The repression of the Gezi protesters, the systematic targeting of the CHP, HDP, and Gülen-affiliated individuals, and the deployment of conspiratorial discourse around elections and national crises illustrate how SDIOs are integral to the authoritarian toolkit. These operations not only reshape public perceptions but also directly threaten democratic principles such as pluralism, accountability, and freedom of expression.

Turkey's experience thus serves as a microcosm of a broader global phenomenon, wherein digital tools are weaponised to manipulate information ecosystems and destabilise democracies from within. As governments, civil society actors, and international institutions confront this challenge, cultivating digital literacy, fostering resilient information environments,

and safeguarding spaces for democratic dialogue are essential. The ability to discern fact from fabrication is no longer simply a matter of individual vigilance – it is a collective imperative for democratic survival.

Funding: This work was supported by Australian Research Council [Grant Number DP230100257]; Gerda Henkel Foundation [Grant Number AZ 01/TG/21]; Australian Research Council [Grant Number DP220100829].

References

Ablak, Ersu. (2022). "CHP'nin trol raporu ve Türkiye'de ve dünyada trol düzeni." *Yetkin Report*. February 8. https://yetkinreport.com/2022/02/08/chpnin-trol-raporu-ve-turkiyede-ve-dunyada-trol-duzeni/ (accessed on October 29, 2023).

Akca, D., Ozeren, S., Onat, I. and Cubukcu, S. (2021). "Political Astroturfing in Twitterscape: The Role of Troll Armies in Turkey's democratic backsliding." *Orion Policy Institute*. July 28. https://www.orionpolicy.org/research/44/political-astroturfing-in-twitterscape-the-role-of-troll-armies-in-turkeys-dem (accessed on October 27, 2023).

Akis, Fazıl Alp. (2022). "Turkey's troll networks." *Heinrich Böll Stiftung*. March 21. https://eu.boell.org/en/2022/03/21/turkeys-troll-networks (accessed on October 28, 2023).

Albayrak, Ayla and Parkinson, Joe. (2013). "Turkey's government forms 6,000-member social media team." *The Wall Street Journal*. https://www.wsj.com/articles/SB10001424127887323527004579079151479634742 (accessed on October 17, 2023).

Bozkurt, Abdullah. (2022). "Turkish hacker who stole a critic's Twitter account granted impunity by the government." *Nordic Monitor*. January 6. https://nordicmonitor.com/2022/01/turkish-hacker-who-stole-twitter-account-of-a-critic-awarded-impunity-by-government/ (accessed on November 1, 2023).

Bulur, Sertac. (2022). "EGM: Mayıs'ta 145 milyon tweet paylaşılan hesapların yüzde 23'ü bot hesap." *Anadolu Ajansı*. June 7. https://www.aa.com.tr/tr/gundem/egm-mayista-145-milyon-tweet-paylasilan-hesaplarin-yuzde-23u-bot-hesap/2607433 (accessed on October 23, 2023).

Burke, Barbara Ruth and Şen, Ayşe Fulya. (2018). "Social media choices and uses: Comparing Turkish and American young-adults' social media activism." *Palgrave Communications*. https://doi.org/10.1057/s41599-018-0090-z

Cyber Intelligence Contest. (2021). "Cyber intelligence contest." *Digital Transformation Office of the Presidency of Turkey*. https://cbddo.gov.tr/en/projects/cyberintelligencecontest/ (accessed on October 17, 2023).

Daily Motion. (2020). "Mahir Ünal: AKP olarak 2 milyon 100 bin kişiyle sosyal medyada bulunuyoruz." *Daily Motion*. https://www.dailymotion.com/video/x7wa40e (accessed on October 28, 2023).

Elmas, Tugrulcan. (2023). "Analyzing activity and suspension patterns of Twitter bots attacking Turkish Twitter trends by a longitudinal dataset." *arXiv.org*. https://doi.org/10.1145/3543873.3587650

Elmas, Tuğrulcan, Overdorf, R., Özkalay, Ahmed Furkan and Aberer, K. (2019). "Ephemeral astroturfing attacks: The case of fake Twitter trends." *arXiv: Cryptography and Security*. October 17. https://www.researchgate.net/profile/Tugrulcan-Elmas-2/publication/336638958_Ephemeral_Astroturfing_Attacks_The_Case_of_Fake_Twitter_Trends/links/5f45723c92851cd3022cd323/Ephemeral-Astroturfing-Attacks-The-Case-of-Fake-Twitter-Trends.pdf

The Express Tribune. (2016). People Think Lindsay Lohan Is Being Paid by the Turkish Govt, *The Express Tribune*, 4 November 2016. URL: https://tribune.com.pk/story/1220440/people-think-lindsay-lohan-paid-turkish-govt

Fixler, Annie. (2023). "Cyber resilience helps democracies prevail against authoritarian disinformation campaigns." *Foundation for Defense of Democracies/Digital Front Lines*. June 14. https://www.fdd.org/analysis/2023/06/14/cyber-resilience-helps-democracies/ (accessed on September 11, 2023).

Gazeteport. (2016). "Küfür TT'si." *Gazeteport*. April 6. https://gazeteport.com/2016/kufur-ttsi-36059/ (accessed on October 29, 2023).

Goud, Naveen. (2018). "Turkey hackers sneak into social media accounts of US Journalists." *Cyber Security Insiders*. https://www.cybersecurity-insiders.com/turkey-hackers-sneak-into-social-media-accounts-of-us-journalists/ (accessed on November 1, 2023).

Grossman, Shelby, Akis, Fazil Alp, Alemdaroğlu, Ayça, Goldstein, Josh, A. and Johnson, Katie. (2020). "Political retweet rings and compromised accounts: A Twitter influence operation linked to the youth wing of Turkey's ruling party." *Stanford Internet Observatory*. June 11. https://fsi9-prod.s3.us-west–1.amazonaws.com/s3fs-public/20200611_turkey_report.pdf

Gulseven, E. (2021). "Identity, nationalism and the response of Turkey to COVID-19 pandemic." *Chinese Political Science Review* 6(1): 40–62. https://doi.org/10.1007/s41111-020-00166-x. Epub 2020 Nov 27. PMCID: PMC7693851.

Hern, Alex. (2017). "Twitter accounts tweet swastikas and pro-Erdoğan support in massive hack." *The Guardian*. March 15. https://www.theguardian.com/technology/2017/mar/15/twitter-turkey-accounts-hack-tweet-swastikas-pro-erdogan (accessed on November 1, 2023).

HRW. (2023). "Questions and answers: Turkey's control of the internet and the upcoming election." *Human Rights Watch (HRW)*. May 10. https://www.hrw.org/news/2023/05/10/questions-and-answers-turkeys-control-internet-and-upcoming-election#_Toc134065370 (accessed on October 29, 2023).

Hull, Justina. (2023). "Turkiskt hackerforum manar till attacker mot svenska banker." *SVT*. January 27. https://www.svt.se/nyheter/inrikes/turkiskt-hackerforum-manar-till-attacker-mot-sverige (accessed on November 1, 2023).

Humprecht, E., Esser, F. and Van Aelst, P. (2020). "Resilience to online disinformation: A framework for cross-national comparative research." *The International Journal of Press/Politics* 194016121990012. https://doi.org/10.1177/1940161219900126

Hurriyet Daily News. (2023). "87 pct of Turkish people use internet in 2023." *Hurriyet Daily News*. August 30. https://www.hurriyetdailynews.com/87-pct-of-turkish-people-use-internet-in-2023–185872#:~:text=87%20pct%20of%20Turkish%20people%20use%20internet%20in%202023%20%2D%20Türkiye%20News (accessed on October 23, 2023).

Hurriyet Daily News. (2013). "Turkish prime minister vows to increase police force." *Hurriyet Daily News*. June 19. https://www.hurriyetdailynews.com/turkish-prime-minister-vows-to-increase-police-force-49006 (accessed on October 28, 2023).

Hurriyet Daily News. (2021). "Registrations open for Hack Istanbul 2021 contest." *Hurriyet Daily News*. May 6. https://www.hurriyetdailynews.com/registrations-open-for-hack-istanbul-2021-contest-164490 (accessed on November 2, 2023).

Hutchinson, Sophie. (2013). "Social media plays major role in Turkey protests." *BBC*. June 4. https://www.bbc.com/news/world-europe-22772352 (accessed on October 28, 2023).

Idiz, Semih. (2013). "Erdogan places blame for protests on international conspiracy." *Al-Monitor*. June 14. https://www.al-monitor.com/originals/2013/06/erdogan-gezi-

conspiracy-taksim-governance-authoritarian-akp.html#ixzz8HRVsnyn1 (accessed on October 28, 2023).
Karakaya-Polat, Rabia. (2018). "Religious solidarity, historical mission and moral superiority: Construction of external and internal 'others' in AKP's discourses on Syrian refugees in Turkey." *Critical Discourse Studies* 2. https://doi.org/10.1080/17405904.2018.1500925
Karatas, Duygu and Saka, Erkan. (2017). "Online political trolling in the context of post-Gezi social media in Turkey." *International Journal of Digital Television* 8(3): 383–401. https://doi.org/10.1386/jdtv.8.3.383_1
Kenes, Bulent. (2020). *A Genocide in the Making?* Clifton, NJ: Blue Dome Press.
Kiniklioglu, Suat. (2017). "Turkey and Russia: Aggrieved Nativism par excellence." *The Turkey Analyst*. May 10. http://www.turkeyanalyst.org/publications/turkey-analyst-articles/item/582-turkey-and-russia-aggrieved-nativism-par-excellence.html (accessed on October 25, 2023).
Korkmaz, Seren Selvin. (2023). "Polarizing populism vs. inclusive positivity: Erdoğan and Kılıçdaroğlu's dueling campaign strategies." *MEI*. May 8. https://www.mei.edu/publications/polarizing-populism-vs-inclusive-positivity-erdogan-and-kilicdaroglus-dueling-campaign (accessed on October 31, 2023).
Lancaster, Caroline. (2014). "The iron law of Erdogan: The decay from intra-party democracy to personalistic rule." *Third World Quarterly* 35(9): 1672–1690. https://doi.org/10.1080/01436597.2014.970866
Lessenski, Marin. (2023). "The media literacy index – 'bye bye birdie': Meeting the challenges of disinformation." *European Policies Initiative*. Open Society Institute. https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English–22.06.pdf
Levinger, M. and Lytle, P. F. (2001). "Myth and mobilisation: The triadic structure of nationalist rhetoric." *Nations and Nationalism* 7(2): 175–194. https://doi.org/10.1111/1469-8219.00011
Marschall, Melissa and Konak-Unal, Saadet. (2021). *Media Bias, Kurdish Repression, and the Dismantling of Local Democracy in Turkey*. Working Paper No. 39. https://gld.gu.se/media/2053/gld-working-paper–39.pdf
Marwick, A. and Lewis, R. (2017). *Media Manipulation and Disinformation Online*. New York, NY: Data & Society Research Institute. https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf
Minto, Rob. (2023). "How Turkey's government gamed Twitter." *Newsweek*. May15.https://www.newsweek.com/twitter-turkey-content-removal-pro-government-accounts-1800328 (accessed on September 11, 2023).
Nefes, Türkay Salim. (2017). "The impacts of the Turkish government's conspiratorial framing of the Gezi Park protests." *Social Movement Studies* 1–13. https://doi.org/10.1080/14742837.2017.1319269
Poole, Thom. (2022). "Osman Kavala: Turkish activist sentenced to life in prison." *BBC*. April 26. https://www.bbc.com/news/world-europe-61218241 (accessed on October 31, 2023).
Selcuki, Can. (2023). "Why Turkish pollsters didn't Foresee Erdogan's win." *Foreign Policy*. June 7. https://foreignpolicy.com/2023/06/07/turkey-elections-polls-erdogan-kilicdaroglu/#cookie_message_anchor (accessed on October 12, 2023).
Souli, Sarah. (2018). "Turkey's band of pro-Erdoğan hackers keep trolling Europe." *Vice*. March 17. https://www.vice.com/en/article/wj7enx/turkeys-band-of-pro-erdogan-hackers-keep-trolling-europe (accessed on November 1, 2023).
Tahiroglu, Merve. (2021). "Erdoğan uses tragic killings to criminalize Kurdish politics, civil society." *POMED*. February 19. https://pomed.org/publication/erdogan-uses-tragic-killings-to-criminalize-kurdish-politics-civil-society/ (accessed on October 29, 2023).

Topcu, Gulsen. (2020). "IHH'dan Gazze ablukasına karşı sosyal medya kampanyası." *Anadolu Ajansı*. May 21. https://www.aa.com.tr/tr/dunya/ihhdan-gazze-ablukasina-karsi-sosyal-medya-kampanyasi-/1848648 (accessed on October 23, 2023).

Turk, H. Bahadir. (2018). "'Populism as a medium of mass mobilization': The case of Recep Tayyip Erdoğan." *International Area Studies Review* 223386591876111. https://doi.org/10.1177/2233865918761111

Unker, Pelin. (2023). "Twitter'da beş gündem etiketinden biri sahte." *DW Türkçe*. May 12. https://www.dwturkce.com/tr/twitterda-seçim-manipülasyonu-beş-gündem-etiketinden-biri-sahte/a-65345776 (accessed on October 17, 2023).

Yesil, Bilge, Sozeri, Efe Kerem and Khazraee, Emad. (2017). "Turkey's Internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance." *Internet Policy Observatory*. February 28. https://repository.upenn.edu/internetpolicyobservatory/22 (accessed on November 1, 2023).

Yildiz, E. and Smets, K. (2019). "Internet trolling in 'networked' authoritarianism: A qualitative content analysis of tweets by regime supporters and 'Ak Trolls' in July 2016." *Middle East Journal of Culture and Communication* 12(3): 348–368. https://doi.org/10.1163/18739865-01203003

Yilmaz, I. (2021). *Creating the desired citizen: Ideology, state and Islam in Turkey*. Cambridge University Press.

Yilmaz, I., Caman, M. E. and Bashirov, G. (2020). How an Islamist party managed to legitimate its authoritarianization in the eyes of the secularist opposition: The case of Turkey. *Democratization* 27(2): 265–282. https://doi.org/10.1080/13510347.2019.1679772

Yilmaz, I. and Shipoli, E. (2022). "Use of past collective traumas, fear and conspiracy theories for securitization of the opposition and authoritarianisation: The Turkish case." *Democratization* 29(2): 320–336.

Yilmaz, Ihsan, Akbarzadeh, Shahram and Bashirov, Galib. (2023a). "Comprehending the tactics of strategic digital information operations (SDIOs)." *Populism & Politics (P&P)*. European Center for Populism Studies (ECPS). September 10. https://doi.org/10.55271/pp0024

Yilmaz, I., Shipoli, E. and Demir, M. (2023b). *Securitization and authoritarianism: The AKP's oppression of dissident groups in Turkey*. Palgrave Macmillan Singapore.

Yılmaz, Z. and Turner, B. S. (2019). "Turkey's deepening authoritarianism and the fall of electoral democracy." *British Journal of Middle Eastern Studies* 46(5): 691–698. Routledge eprint. https://doi.org/10.1080/13530194.2019.1642662

8

INDIA'S STRATEGIC DIGITAL INFORMATION OPERATIONS

Ihsan Yilmaz and Chloe Smith

Introduction

Over the past decade, India has witnessed a profound transformation in state–society relations in the digital sphere. Once heralded for its "Digital India" initiative – a vision promising open access, innovation, and democratic connectivity – India has instead evolved into a notable case study in digital authoritarianism. Under the leadership of Prime Minister Narendra Modi and the Bharatiya Janata Party (BJP), the state has aggressively asserted control over cyberspace, deploying a sophisticated array of SDIOs to manage dissent, dominate narratives, and consolidate power.

Far from being incidental or reactive, India's SDIOs constitute a deliberate, systematised strategy. Through extensive surveillance, content takedowns, legal repression, and orchestrated disinformation campaigns, the government has transformed the internet from a platform for public deliberation into a tightly policed space that reinforces ideology. These operations are carried out through a blend of formal state institutions, regulatory mechanisms, state-aligned media, and shadow digital actors – including bot networks, troll armies, and partisan influencers – who operate in synchrony to amplify the regime's messaging and marginalise dissent.

This chapter offers a comprehensive analysis of India's domestic SDIOs and their broader implications. The first section briefly identifies general characteristics of the BJP's SDIOs: Legal and regulatory frameworks that empower censorship and undermine accountability; internet shutdowns and social media content removals becoming a normalised instrument of political control; the use of digital and informational manipulation strategies such as bots and trolls; and emotional, identity-based mobilisation strategies – centered

DOI: 10.4324/9781003628088-11
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

around Hindu nationalism (Hindutva) – being deployed to polarise society, delegitimise opposition, and manipulate digital information to maintain hegemony. The second section of the chapter maps the application of SDIOs by the BJP using four significant recent events: the 2020–2021 farmers' protests, 2020 Delhi riots, COVID-19 "infodemic," and the 2019 and 2024 election disinformation campaigns.

General Characteristics of Domestic SDIO Campaigns in India

The BJP SDIO infrastructure is significant and far-reaching. Although not comprehensive, this chapter highlights several pertinent SDIO features used by the BJP and their development in the Indian government's agenda.

Propaganda Campaigns via State-Aligned Media

The BJP benefits from a media ecosystem that has increasingly supported its political discourse, blurring the line between independent journalism and state propaganda. Over the past decade, many of India's television news channels and print outlets have adopted a markedly pro-BJP position. One sign of an increasingly homogenised media environment is India's plummeting press freedom ranking. In 2023, Reporters Without Borders ranked India 161st of 180 countries – an even more diminished ranking than previous years – citing the reason "media takeovers by oligarchs close to Prime Minister Modi have jeopardised pluralism" (Reporters Without Borders, 2023a, 2023b).

A mutually beneficial situation drives this alignment: "state-aligned media" entities pick up and broadcast narratives initially propagated on social media by BJP influencers, legitimising and propelling these narratives forward. Their coverage is then aggressively amplified online by the BJP's troll armies (Mohan, 2021; Bloomberg, 2024). Meanwhile, ostensibly private pro-government news sites have proliferated online. Portals like OpIndia, Swarajya, and The Frustrated Indian brand themselves as alternative media but often function as propaganda machines, generating a significant number of misleading reports favoring the BJP and maligning its opponents (Bhat, 2023).

India's media and digital spheres are an increasingly vital component in the government's propaganda apparatus. Although independent journalism still exists (investigative outlets like The Wire, Scroll, or Caravan have broken important and critical stories), they face ongoing threats of legal cases and raids (Human Rights Watch, 2022a, 2022b), resulting in a chilling effect.

Government Control and Censorship Legislation

The Modi government has systematically fortified its legal and institutional arsenal to police the digital sphere. Following the BJP's 2019 re-election,

officials escalated their digital authoritarianism, clamping down on tech platforms and targeting users deemed troublesome. Armed with expansive legal powers, the Indian state has aggressively moved to censor online content and silence critical voices. The government's enforcement of takedowns accelerated markedly after 2020 (Singh, 2021). By 2021, BJP officials were demanding the removal of hundreds of posts – and, in some cases, entire accounts – that portrayed the regime in a negative light (Singh, 2021). Twitter, Facebook, and YouTube received orders to take down content related to the farmer protests, corruption allegations, and other sensitive issues (Ravi, 2021).

In February 2021, the government enacted the new *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, which vastly increased government powers to moderate and remove online material, making India's digital realm "one of the most heavily regulated of any major democracy" (Ellis-Petersen, 2021). Even cautious mainstream media outlets criticised the *2021 Information Technology Rules*; an editorial in *The Hindu*, for instance, dubbed them "a wolf in watchdog's clothing" that would give authorities "a good deal of leverage over online news publishers" (The Hindu, 2021).

The *Information Technology Rules* also crucially target social media organisations and, in some cases, their users. Platform executives face legal repercussions, including the threat of arrest, for non-compliance with government directives. This has created a climate of fear and proactive censorship within the tech industry. For example, Twitter's offices in Delhi were infamously subjected to police harassment after the platform fact-checked a tweet from a BJP spokesperson (Athrady, 2021), signaling that non-cooperation could invite punitive action. Part of this legislation includes the removal of laws that had previously shielded intermediaries from liability for user-generated content. Consequently, the state has empowered itself to target online critics without due judicial process (Freedom House, 2022). The Ministry of Home Affairs even launched a cybercrime volunteer program in 2021 that encourages loyal citizens to report "unlawful content" harmful to India's integrity or social fabric. Crowdsourced digital surveillance such as this blurs the line between state and vigilante action, expanding the reach of institutional repression.

In 2023, the government made even more repressive amendments to the *Information Technology Rules,* mandating platforms to pre-emptively block or flag content deemed a threat to public order, decency and morality, national security, or any content deemed as "fake news" by the government (Amnesty International, 2023). The government also proposed an amendment that would empower a designated fact-checking unit – operating under the Ministry of Electronics and Information Technology – to unilaterally label any unfavorable online content about the government as "fake or false," and compel its removal (Panijar and Waghre, 2023). In practice, this

framework gives the regime broad discretion to censor and outlaw online speech that do not conform to its political position, with minimal transparency or oversight (Reuters, 2023).

The cumulative effect of these laws and regulations is to create a legal-institutional framework for digital authoritarianism (Yilmaz and Saleem, 2022). By making private companies and even ordinary internet users responsible for enforcing state directives (under threat of punishment), the government has effectively outsourced and normalised censorship as part of its governance structure.

Internet Shutdowns, Social Media Removal Requests

The frequency of shutdowns in India is unparalleled. According to monitoring by digital rights groups, as of 2023, India had led the globe in the number of internet shutdowns for six consecutive years (Kaskar, 2024). Access Now (2022) reported that in 2023 alone, Indian authorities imposed at least 116 internet shutdowns – by far the highest of any other country.

The official rationale provided for such shutdowns is to prevent the spread of rumors and disinformation and the organising of violence (Human Rights Watch, 2023). In practice, these blackouts often target regions facing significant protests, political instability, or ethnic conflict. They are also an extreme measure to prevent backlash against the government. For example, BJP politicians and aligned actors have been found to use WhatsApp and Facebook to circulate provocative misinformation painting Muslims or other minorities as threats to public safety, contributing to outbreaks of violence (Ruijgrok, 2021). Then, rather than punishing the perpetrators of hate speech, authorities frequently respond by denying internet access to entire districts or states, thereby silencing any responding voices on the matter (Freedom House, 2024).

The blanket denial of internet access effectively amounts to the collective punishment of entire populations and the suppression of information about possible state abuses. Beyond the economic and social costs of internet shutdowns, which are enormous, they represent a serious curtailment of fundamental democratic rights – a blunt denial of the public's ability to know, to speak, and to assemble (in both the digital and physical sense).

Another central pillar of India's digital information strategy involves the censorship and control of social media platforms. The volume of content removal requested by Indian authorities presents another staggering picture: India leads the world in such requests, far exceeding the number of even full-scale authoritarian countries (Freedom House, 2021). The Modi government has leveraged legal and regulatory tools like those detailed earlier to compel companies like Twitter (now X), Facebook, and YouTube to remove content and restrict accounts that are deemed critical of the state or sympathetic to causes

the regime does not support (Ravi, 2021). Over the past few years, authorities have sent an avalanche of takedown requests to social media firms and introduced new rules to tighten governmental oversight of online content (Ahmed, 2023). These efforts amount to a concerted campaign to neutralise social media, diminishing the possibility of platforms being a space for dissent, and to ensure compatibility between online and BJP narratives. Takedown demands, backed by the threat of legal sanctions, contribute to an overall chilling effect that deters users from voicing dissent in the first place.

Digital Manipulations: State-Aligned Troll Armies, Bot Networks, and Disinformation/Conspiracy Campaigns

Over the past decade, the BJP and its affiliates have developed a sophisticated digital apparatus to flood social media with propaganda and disinformation, troll the opposition, and amplify and disseminate BJP-approved messaging. At the heart of this apparatus is the party's IT cell – a dedicated team, reportedly numbering in the hundreds of thousands when extended to volunteers, that coordinates content creation and dissemination across platforms. This incorporates official social media teams as well as a vast ecosystem of sympathetic influencers, paid trolls, bot networks, and fake accounts that can be mobilised in response to political moments (Yilmaz and Saleem, 2022).

At the heart of digital manipulations is a concerted and multifaceted effort by those in or seeking power to control the information that is accessible and prioritised for targeted or entire audiences. The mechanics of India's digital information strategies often mirror those seen in other authoritarian contexts, although they have distinctly local innovations. Inauthentic digital activity – ranging from automated bots to hijacked or pseudonymous accounts – has become a central feature of electoral politics in India. The ruling party has been especially effective in leveraging these tactics, deploying "WhatsApp vigilantes" or "IT armies" to do the work of disseminating rumors and conducting smear campaigns. The BJP's model of online campaigning, combining organic supporters with trolls and fake personas, has been emulated to some extent by other parties, but they are unable to match the scale and sophistication of the ruling party's operation (Jaswal, 2024; Mahapatra and Plagemann, 2019).

In recent years, social media platforms have improved detection of automated bots. For instance, in 2020, Twitter acknowledged that it had removed over a thousand accounts tied to a BJP-backed network manipulating the platform (Twitter Safety, 2020). Facebook and Instagram have similarly taken down clusters of pages engaging in "coordinated inauthentic behavior". Yet independent researchers have found that as these detection mechanisms improved, government affiliates have shifted to engaging real humans using fake profiles. This leverages grassroots participation to manufacture

consensus, making it appear as though large numbers of ordinary Indians are enthusiastically replicating the government's discourse online.

Emotional and Identity-Based Mobilisation Strategies

A core pillar of BJP's SDIOs is the strategic dissemination of emotive, (religious) identity-driven narratives to shape public opinion. The party and its aligned influencers have effectively harnessed Hindu nationalist (Hindutva) rhetoric online. This fosters a common identity (Hindu) and mobilises support online, while portraying critics and opposition as enemies of the Hindutva nation, and scapegoating minority groups for political tensions.

Muslim Indians, the country's largest minority, bear the brunt of this scapegoating. Muslims are often portrayed as the "internal other" and a demographic and religious threat in Hindutva discourse. Social media has become a fertile ground for spreading Islamophobic misinformation and myths, many of which existed offline but now find unprecedented reach (Banaji and Bhat, 2020).

Senior BJP figures like Amit Malviya have disseminated incendiary claims – for example, branding Muslim men as part of "love jihad" plots or implying opponents are secretly aided by Pakistan. Accusations of "Hindu-phobia" have been weaponised online to deflect criticism and mobilise the Hindu majority.

These types of online narratives prove potent in India's SDIO framework due to the construct of social media platform algorithms, which prioritise engagement and tend to favor "sensationalist content that triggers emotional responses" (The Wire, 2023). As a result, Hindutva content tends to be prioritised online (The Wire, 2023).

Modi and the BJP also utilise the emotional appeal of performative religious events and political gatherings to generate interest and loyalty online. This includes Modi performing rituals at massive Hindu religious ceremonies, which are televised and then widely available on YouTube, as well as choreographed border confrontations with neighboring countries that fuel nationalist fervor on digital platforms (Vasudeva, 2025).

Case Studies of Domestic SDIO Campaigns in India

Farmers' Protest (2020–2021): Smearing Dissent and Crushing Solidarity

One of the most significant protest movements in modern Indian history erupted in late 2020, when tens of thousands of farmers camped on Delhi's outskirts to demand the repeal of new agricultural laws. The BJP government's SDIO response to the protests, one of the most substantial challenges

to date to Modi's government (Jain, 2024), combined SDIO strategies of digital repression and propaganda, directly fuelling the mass violence and detainment of protesters and critics that ensued.

The government sought to prevent the farmers' message from gaining traction on social media from the outset. Officials pressured Twitter, Reddit, Facebook, Snap, and Instagram to take down and block pages, links, and accounts sympathetic to the protests (Livemint, 2024). During the height of the farmer protests, for example, authorities demanded that Twitter shut down the accounts of investigative journalists and opposition politicians who were posting news updates and critiques. Internal Twitter communications (later reported by journalists) indicated that the government threatened to arrest the platform's India-based staff if the company did not comply with its account suspension requests (Arora, 2024). Although Twitter initially resisted, it eventually yielded to intense pressure and threats (Al Jazeera, 2024; Dixon, 2021). Although some accounts were later unblocked following public pressure, the episode revealed the state's willingness to enact digital information blackouts to suppress dissent, setting a lasting precedent for compliance.

The BJP's tactics during the mobilisation also previewed a broader approach of using internet shutdowns. Notably, the government suspended internet services at protest sites multiple times. These targeted shutdowns aimed to disrupt communications between protesters and prevent live updates reaching a wider audience (Amnesty International, 2021). They also impeded journalists' ability to cover events on the ground, contributing to a partial information blackout during critical moments of the agitation.

Disinformation campaigns, propelled forward by an extensive real and fake/bot network, sought to undermine the massive farmers' protests of 2020–2021. Protesters were systematically associated with separatists seeking an independent Sikh homeland (Khalistan), terrorism, and anti-nationalism (Iqubbal and Alam, 2021). Content examples on mainstream social media platforms include the misidentification of protesters as known extremists; doctored videos from past protests associating current protesters with terrorist movements; and manipulated photos seeking to foment anti-Sikh sentiment. The breadth of the disinformation was remarkable, ranging from fringe conspiracy theories on obscure blogs to WhatsApp forwards in rural villages, through to State television outlets repeating the falsehoods.

India's media channels were well attuned to these narratives, and coverage reached a crescendo when international celebrities including Rihanna and Greta Thunberg voiced support for the farmers on Twitter in early February 2021 (Mishra et al., 2021). Reactions from the BJP's digital apparatus to this development were swift. The External Affairs Ministry released a statement condemning "foreign individuals" for weighing in on the matter, and BJP activists launched a #IndiaAgainstPropaganda and

#IndiaStandsTogether hashtag trend, linking the celebrity support to conspiracy theories about foreign interference (Mishra et al., 2021). When Greta Thunberg accidentally tweeted a public link to a protest support "toolkit" (an informative document for protesters), the government weaponised the information, claiming it was proof of a ploy to defame – and wage a social, cultural, and economic war on – India (Tiwari, 2021). A young activist who had been involved in editing the toolkit was consequently arrested on sedition charges – a dramatic instance, and warning – of digital support for the protests being criminalised (Tiwari, 2021).

Throughout the protests, pro-BJP trolls engaged in systematic harassment of prominent supporters of the farmers. The social media monitoring site BOOM reported a surge in fake news targeting protest leaders, including doctored photos, that, for instance, portrayed them as violent criminals. Despite significant efforts to discredit the movement, the protesters persevered and gained significant concessions, eventually forcing the government to repeal the farm laws in late 2021. However, the digital campaign against the movement set a harmful precedent because it was one of the first and most overt times the government made an attempt to mass censor the social media accounts of a domestic movement. This made clear the lengths to which the state would go to suppress online mobilisation.

The farmers' protest case is a demonstrative case of a digital authoritarian regime deploying the full spectrum of SDIO tools on its own citizens, including censorship (e.g., platform pressure and internet shutdowns), disinformation (e.g., widely disseminating claims that protesters are terrorists), legal reprisal (e.g., arresting toolkit sharers), and emotional manipulation (e.g., encouraging nationalist fervor against protesters and supporters). It underlined how digital authoritarianism strategies can be used even in an ostensibly democratic and peaceful movement to counter a popular challenge to government policy.

Delhi Riots (February 2020): Online Hate Triggering Offline Violence

The Delhi riots of February 2020 are a grim case study that demonstrates how sustained online hate campaigns can manifest in offline violence – aligning the state's response (or lack thereof) with SDIO strategies of demonising victims and shielding perpetrators on digital platforms.

In the months before the riots, Delhi had been one of the epicenters of peaceful protests against the passing of the controversial Citizenship Amendment Act (CAA), which makes religion the criterion for citizenship and specifically excludes Muslim populations. Following an intensive online campaign against the protests, a period of violence erupted in India's capital, resulting in the deaths of at least 53 people, an additional 500 estimated injured, properties destroyed, and entire communities displaced by targeted

attacks by mobs (Kaul and Lakhera, 2025). A small number of those killed were Hindus. However, most victims were Muslim (Human Rights Watch, 2020).

A fact-finding committee described the BJP's rhetoric in the lead-up to, and following the passing of the Citizenship Amendment Act, as "divisive and inflammatory," contributing to the volatile environment in which the riots broke out (Iyer, 2022). Numerous BJP leaders were "vociferous in their positions against the anti-CAA protests," and used social media platforms extensively to spread their views (Citizens Committee, 2022). Social media discourse before and during the riots was similarly characterised by misinformation about the protests and hatred toward the protesters. Among the inflammatory WhatsApp messages being forwarded were "how to spot 12 signs of jihad," calls for economic boycott of Muslims, and Muslim migration into Uttarakhand and Uttar Pradesh (Nair, 2021).

Some of the most incendiary posts were traced to profiles affiliated with far-right Hindu organisations, including individuals who followed or were followed by BJP figures (Scroll.in 2020). BJP party leaders and candidates labeled protesters as "traitors," resulting in widespread circulation of the slogan "goli maaro" (shoot the traitors) on traditional and social media platforms (Citizens Committee, 2022). Even when the content did not originate from BJP sources, they were supported and legitimised by the government first, implicitly when the government did not respond to their influence on the riots, and second, explicitly when BJP members or Modi followed or endorsed the authors on social media (Mohsina, 2020).

The aftermath of the riots witnessed an increased legislative commitment to SDIO. For instance, the Delhi police filed 18 "politically motivated charges" against activists, students, residents, and political opponents – 16 of whom are Muslims (Human Rights Watch, 2022b). Police charges relied on weak testimonies and WhatsApp chats, as well as social media communication that informed about and organised peaceful protests (Human Rights Watch, 2022b). Social media platforms were not held to account for their role in the riots. During the Delhi riot hearings, Facebook was interrogated by a parliamentary committee over its role, resulting in its representatives admitting that ruling party figures had indeed violated policies but largely remained online (Indian Express, 2021).

The Delhi riots provide a crucial study of how SDIOs can be used as a layered and rapid response during a crisis. First, pro-government hate propaganda proliferated online primes an environment for violence, namely the dehumanisation of a community and rallying of a majority. Second, during the conflict, digital tools aid those instigating or encouraging the violence, for example, WhatsApp is used for coordination and spreading rumors about what is happening in real time. Third, disinformation is used to rewrite the account after the fact, casting blame on victims or dissidents. Fourth and

finally, the state uses legal and media channels to reinforce this false account, while silencing those who attempt to tell the real story.

The riots are a concerning example of how thoroughly the lines between reality and propaganda can blur in the age of social and digital media – and how an authoritarian-leaning state leverages this to its advantage. Importantly, they are also a grim case study of how sustained online hate campaigns can contribute to the eruption of communal violence – and how the state's response (or lack thereof) aligns with SDIO functions of demonising victims and shielding perpetrators on digital platforms.

COVID-19 "Infodemic" (2020–2021): Communalising a Public Health Crisis

The onset of the COVID-19 pandemic posed a crisis of governance for India, in which the ruling party opportunistically reshaped the narrative through disinformation strategies and scapegoating. The early phases of the pandemic saw a surge of Islamophobic propaganda online blaming Muslims for spreading the virus – illustrating how the BJP's ecosystem instrumentalises available issues and events to reinforce populist Hindutva narratives.

When COVID-19 cases began rising in March 2020, an outbreak cluster at an Islamic missionary gathering (Tablighi Jamaat) was seized upon by BJP-aligned social media actors to escalate a hate campaign blaming Muslims for the spread of the virus or being "super spreaders." Almost overnight, hashtags like #CoronaJihad and #BioJihad trended, linked to conspiracy theories widely shared on social media that Muslims were deliberately disregarding lockdowns and infecting Hindus (Tieri and Ranjan, 2023; Awan et al., 2024). The scope of these digital disinformation campaigns is extraordinary: The digital human rights group Equity Labs found that Tweets with #*CoronaJihad* appeared nearly 300,000 times, reaching up to 165 million users between March 28 and April 3, 2020 (Tieri and Ranjan, 2023).

The false narrative of a Muslim plot to infect India was amplified by BJP members, supporters, and even some mainstream TV channels. The tacit scapegoating of Muslims by officials gave credibility to misinformation and disinformation, with dire consequences offline: Muslims across India faced boycotts, harassment, and denial of medical care, resulting in further unnecessary deaths (Awan et al., 2024).

The BJP government were criticised for their "frantic" attempts to control all aspects of information about the crisis (Reporters Without Borders, 2020). This included traditional and digital reporters being denied access to public health information; the government attempting to force journalists to publish only information that it had approved; arresting and detaining those who did speak out against the Indian state; and sustained online hate

campaigns against critical voices orchestrated by the BJP and their online activists (Reporters Without Borders, 2020).

Any criticism about the government's (mis)management of the pandemic, such as the reported export of vaccines amid domestic scarcity, was met with counter-narratives that critics were unpatriotic or spreading fear. For instance, during India's devastating second wave in April 2021, dozens of individuals who tweeted pleas for oxygen or criticised authorities were targeted by the police under various laws, as local officials were accused of seeking to stifle "negative" information rather than address the crisis (BBC News, 2021).

The COVID-19 infodemic in India had two sides. The first was a disinformation strategy that emotively scapegoated the Muslim minority as responsible for the spread of the virus, and the second was a systematic censorship effort to control the BJP's image. Both served to divert accountability – the former by shifting public anger toward Muslims rather than the mishandling of the outbreak by officials, and the latter by suppressing any voices that did criticise the state's management of the pandemic.

The human cost of the infodemic was high: the spread of divisive narratives about the pandemic deepened societal polarisation and created a discriminatory public health response. The strategic silencing of opposition and censorship of the situation undermined democracy in India and further cemented the government's willingness to operationalise digital authoritarianism to control public discourse.

This case exemplifies how SDIO tactics can be instrumentalised during a national crisis – in this case, a public health emergency – with dire consequences, and how an authoritarian-leaning regime prioritises narrative control over transparency, reputation, and hegemony maintenance over public health and safety.

Electoral Influence and Disinformation (2019 and 2024): Manipulating Voters at Scale

General elections in the world's largest democracy are enormous exercises, and social media has become indispensable to campaigning in India. The BJP has been at the forefront of this digital electioneering, utilising digital platforms as vehicles for propaganda mis- and disinformation, giving the party an edge over less tech-forward and resource-rich rivals. The last two elections, in particular, 2019 and 2024, showcased the party's sophisticated use of SDIO techniques domestically to shape voter perceptions.

The 2019 general election, which the BJP won in a landslide, was dubbed the "WhatsApp election" due to the platform's immense reach in Indian society and the BJP's strategic use of the platform to influence a large number of voters (Bengani, 2019). The BJP reportedly enrolled millions of

volunteers into WhatsApp groups and utilised data analytics to segment voters and disseminate tailored messages (Campbell-Smith and Bradshaw, 2019). Although many of these messages consisted of benign campaigning material, a significant portion were found to communicate misinformation aimed at influencing attitudes, from exaggerated claims of government achievements to scare-mongering about the opposition's policies and plans for the nation. For example, viral WhatsApp forwards falsely claimed the opposition Congress party would remove Hindu temples, while others claimed that voting for Congress meant voting for Pakistan (Poonam and Bansal, 2019).

Emotive Hindutva discourse also intensified in the election seasons. For example, one narrative spread in North India on WhatsApp in 2019 falsely claimed that opposition leaders held secret meetings with a radical Muslim cleric to "plan Islamic law implementation," attempting to consolidate Hindu votes for the BJP. During the 2019 general election, for instance, an array of covert BJP-linked Facebook pages and Twitter handles flooded the platform with vitriolic disinformation targeting opposition leaders. Posts with fabricated quotes falsely attributed to opposition figures, bogus accusations of corruption, and doctored images suggesting rival politicians were "anti-Hindu" proliferated across social media (DFRLab, 2019). These reports also found that fact-checkers struggled to keep pace with the torrent of false claims. Although many of these dubious pages were not immediately connected to the BJP, investigative reports later traced them back to BJP IT cell operatives and consultants.

By the 2024 general election, the digital battlefield had evolved even further. Election campaigning moved beyond the common platforms X, Facebook, and WhatsApp and was also performed on YouTube and other short-video channels – a savvy digital move which researchers identify as instrumental in their success (Rajvanshi, 2024a, 2024b).

New developments, notably AI-generated images and videos ("deepfakes"), entered Indian campaigns. Fabricated videos showing popular film stars endorsing a specific party were disseminated online, while in others, the voices of leaders were cloned to speak in multiple languages (Anadi, 2024). Reports also emerged of deepfakes used by BJP candidates to send personalised appeals to voters in different dialects, while images and videos discrediting opposition leaders were circulated (Dhanuraj et al., 2024). Such BJP content blanketed social media platforms, often significantly outpacing opposition content in volume and virality. Civil society watchdogs found that election ads approved by Facebook and YouTube contained egregious misinformation and even hate speech and were mostly attributed to BJP-aligned entities (Ellis-Petersen, 2024). The lack of platform enforcement following these findings gave BJP propagandists free rein to experiment with new forms of misleading content.

In summary, India's recent elections illustrate the normalisation of organised disinformation as a campaign strategy. The BJP's superior organisation online paired with its access to digital technologies created an uneven playing field in information dissemination during the most recent (2019 and 2024) election campaigns. Disinformation strategies became a prominent feature of political messaging, further distorting the playing field. Additionally, while opposition parties have also leveraged the affordances of social media campaigning, they cannot compete with the BJP's ecosystem of devoted volunteers, ideologically driven content creators (including those in the diaspora, although not covered here), and sympathetic media channels that amplify their narratives. This asymmetry means that the ruling party can set the agenda of electoral debate – often around emotive, divisive issues – far more effectively than its opponents. In democratic terms, this undermines the ideal of informed voting based on factual programs and policies, skewing it toward a state in which voting is influenced by the manipulation of emotions, identities, and a complex and overwhelming information landscape.

Conclusion: Threatened Democratic Discourse, Civil Liberties, and Social Cohesion

As democracies around the world confront the challenge of balancing digital governance with fundamental user rights, India's trajectory raises urgent concerns. It indicates not merely an erosion of freedoms but the institutionalisation of a governance model in which digital tools are weaponised in service of authoritarian and majoritarian rule. This chapter situates India within a growing cohort of democratically elected regimes that are increasingly autocratic in their digital practices – offering a warning about how technological infrastructures, once seen as liberatory, can be harnessed to entrench authoritarianism from within.

The deployment of domestic SDIOs by the BJP has had a deep and troubling impact on India's democratic institutions. By asserting dominance over the digital public sphere, the government has systematically muted dissent, shaped public perception, and promoted a narrative that consistently aligns with its political objectives.

The widespread circulation of propaganda and disinformation has significantly eroded the quality of public discourse. Instead of fostering informed debate, digital platforms are often flooded with emotionally charged and polarising content that crowds out serious policy discussion. The result is a communication environment where factual accounts compete with manufactured narratives, voices of opposition either struggle for visibility or are punished for their views, and citizens are increasingly exposed to distorted sociopolitical realities. This distortion contributes to India's declining internet freedom, making meaningful democratic engagement more challenging.

A pervasive atmosphere of fear now surrounds online expression. Journalists, activists, and everyday users self-censor aware that criticising the government can lead to targeted harassment, job loss, or even legal action. The 2021 IT Rules and other recent legislation have only intensified this climate, resulting in a noticeable decline in independent journalism and public commentary. The space for critique has shrunk, and digital platforms – once heralded as democratic equalisers – are now being used as tools to enforce silence.

At a societal level, the continued vilification of Muslims, activists, and intellectuals as enemies of the nation has widened social divisions and legitimised intolerance. Social media echo chambers amplify this hostility, contributing to real-world violence and deepening intergroup distrust. The erosion of mutual respect and civic trust poses a significant threat to India's long-standing commitment to diversity, and rebuilding these bonds will be a generational challenge.

Elections – while procedurally intact – are increasingly influenced by a digital information space shaped by one-sided messaging. When voters are subjected to a stream of information manipulation strategies and the opposition is denied a fair platform, the democratic process is compromised. A genuine contestation of ideas becomes elusive when one side controls the narrative and suppresses alternative viewpoints.

Through its SDIO tactics, the BJP has managed to entrench a style of authoritarian governance without dismantling the formal architecture of democracy. Institutions remain, but their effectiveness is weakened by coordinated digital coercion and narrative control. This form of governance is difficult to challenge because it wears the mask of democratic legitimacy while steadily curbing participatory rights that make democracy meaningful. The BJP's propaganda architecture serves to homogenise public discourse, redefine national identity through Hindutva, and manufacture consent for authoritarian governance. This approach carries serious consequences for the health and longevity of India's democracy as it enables censorship, legitimises disinformation, and erodes pluralism. The Indian case offers an illustrative example of 21st-century digital authoritarianism, in which controlling the narrative becomes the cornerstone of consolidating power.

By blending institutional power with grassroots digital coercion, the BJP has forged a new model of internal information control. This chapter offers a sobering account of how a democratic state can employ sophisticated digital tactics to entrench authoritarian rule, posing urgent questions for civil liberties, press freedom, and the resilience of democratic institutions in the digital age. The case studies presented in this chapter illustrate how these SDIOS are enacted in various ways during pivotal political moments.

As India navigates its future, reclaiming digital space for open dialogue, transparency, and pluralism will be essential. Addressing these trends will

require robust legal safeguards, increased transparency in platform regulation, civic education, and a cross-party commitment to democratic norms. Without such efforts, the erosion of democratic freedoms in India may continue – quietly, but profoundly.

Funding: This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.

References

Access Now. 2022. "Shattered dreams and lost opportunities: A year of internet shutdowns in India." *Access Now Report*, March.

Ahmed, Rasheed. 2023. "India's Right to Know under threat as social media giants bend to censorship." *Index on Censorship*, September 27. https://www.indexoncensorship.org/2023/09/indias-right-to-know-under-threat-as-social-media-giants-bend-to-censorship/

Al Jazeera, 2024. "India's demand to block accounts amid farmers' stir curtails free speech: X." *Al Jazeera,* February 22. https://www.aljazeera.com/news/2024/2/22/indias-demand-to-block-accounts-amid-farmers-stir-curtails-free-speech-x

Amnesty International. 2021. "India: Government must stop crushing farmers' protests and demonizing dissenters." *Press Release by Amnesty International*, February 9.

Amnesty International. 2023. "India: New Amendment to the Information Technology rules that Threatens Press freedoms must be Withdrawn: Joint statement for World Press Freedom Day." *Amnesty International*, May 2. https://www.amnesty.org/en/wp-content/uploads/2023/05/ASA2067342023ENGLISH–1.pdf

Anadi. 2024. "Deep fakes, deeper impacts: AI's role in the 2024 Indian General Election and beyond." *Global Network on Extremism & Technology*, September 11. https://gnet-research.org/2024/09/11/deep-fakes-deeper-impacts-ais-role-in-the-2024-indian-general-election-and-beyond/

Arora, Suvrat. 2024. "Silenced voices: The battle for free expression amid India's farmer protest." *Al Jazeera Media Institute*, March 17. https://institute.aljazeera.net/en/ajr/article/silenced-voices-battle-free-expression-amid-india's-farmer's-protest

Athrady, A. 2021. "Twitter 'concerned' about India staff safety after police visit; Centre says new rules empower social media users." *Deccan Herald*, May 28. https://www.deccanherald.com/india/twitter-concerned-about-india-staff-safety-after-police-visit-centre-says-new-rules-empower-social-media-users–990558.html

Awan, Imran, Pelham Carter, and Hollie Sutch. 2024. "The blame game: A thematic analysis of islamophobic Tweets during the COVID-19 pandemic." *Ethnic and Racial Studies*, December, 1–19. https://doi.org/10.1080/01419870.2024.2439025

Banaji, Shakuntala, and Ram Bhat. 2020. "How anti-Muslim disinformation campaigns in India have surged during COVID–19." *The London School of Economics and Politics Science (LSE),* December 30. https://blogs.lse.ac.uk/covid19/2020/09/30/how-anti-muslim-disinformation-campaigns-in-india-have-surged-during-covid-19/

BBC News. 2021. "Anger as Twitter ordered to remove critical virus posts." *BBC News*, April 26. https://www.bbc.com/news/world-asia-56883483

Bengani, Priyanjana. 2019. "India had its first WhatsApp election. We have a million messages from it." *Columbia Journalism Review*, October 16. https://www.cjr.org/tow_center/india-whatsapp-analysis-election-security.php

Bhat, Prashanth. 2023. "Hindu-nationalism and media: Anti-press sentiments by right-wing media in India." *Journalism & Communication Monographs*, 25(4), 296–364. https://doi.org/10.1177/15226379231201455

Bloomberg. 2024. "How pro-Modi billionaires are reshaping India's media landscape, 1 outlet at a time: 'Journalism is dead'." https://www.scmp.com/news/asia/south-asia/article/3253214/how-pro-modi-billionaires-are-reshaping-indias-media-landscape-1-outlet-time-journalism-dead

Campbell-Smith, Ualan, and Samantha Bradshaw. 2019. "Global cyber troops country profile: India." Oxford Internet Institute, University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/05/India-Profile.pdf

Citizens Committee. 2022. "Uncertain justice: A citizens committee report on the North East Delhi violence 2020." An initiative of Constitutional Conduct Group (CCG). https://constitutionalconduct.wordpress.com/wp-content/uploads/2022/10/uncertain-justice-citizens-committee-report-on-north-east-delhi-violence–2020.pdf

DFRLab (Digital Forensic Research Lab). 2019. "#GoBackModi vs. #TNWelcomesModi: Coordinated Twitter campaigns in Indian election." *DFRLab, Atlantic Council*, April.

Dhanuraj, D., Sreelakshmi Harilal, and Nissy Solomon. 2024. "Generative AI and its influence on India's 2024 elections: Prospects and challenges in the democratic process." *Policy Paper, Friedrich Naumann Foundation for Freedom*.

Dixon, Robyn. 2021. "Twitter in middle of standoff between Modi Government and free speech advocates." *The Washington Post*, February 9.

Ellis-Petersen, Hannah. 2021. "'Wolf in watchdog's clothing': India's new digital media laws spark fears for freedoms." *The Guardian*, March 11. https://www.theguardian.com/world/2021/mar/11/wolf-in-watchdogs-clothing-indias-new-digital-media-laws-spark-censorship-fears

Ellis-Petersen, Hannah. 2024. "'Revealed' Meta approved political ads in India that incited violence." *The Guardian,* May 20, 2024.

Freedom House. 2021. *Freedom in the World 2021 – India*. Washington, DC: Freedom House.

Freedom House. 2022. *Freedom on the Net 2022: India*. Washington, DC: Freedom House. https://freedomhouse.org/country/india/freedom-net/2022

Freedom House. 2024. *Freedom on the Net 2024: India*. Washington, DC: Freedom House. https://freedomhouse.org/country/india/freedom-net/2024

The Hindu. 2021. "A wolf in watchdog's clothing: On government's move to regulate digital media." *The Editorial, The Hindu,* March 1. https://www.thehindu.com/opinion/editorial/a-wolf-in-watchdogs-clothing-the-hindu-editorial-on-indian-governments-move-to-regulate-digital-media-platforms/article33956670.ece

Human Rights Watch. 2020. "'Shoot the traitors' discrimination against Muslims under India's new citizenship policy." *Human Rights Watch News Release,* April 9.

Human Rights Watch, 2022a. "India: Biased investigations 2 years after Delhi riot." *Human Rights Watch News Release*, February 21.

Human Rights Watch. 2022b. "India: Media freedom under threat." *Human Rights Watch News Release,* May 3.

Human Rights Watch. 2023. "India: Internet shutdowns hurt vulnerable communities." *Human Rights Watch News Release*, June 13.

Indian Express. 2021. "'Undermines media freedom': Editors Guild expresses concern over Centre's new media ethics code." March 6. https://indianexpress.com/article/india/undermine-media-freedom-put-unreasonable-restrictions-editors-guild-expresses-concern-over-centres-new-technology-rules-7216996/

Iqubbal, Asheef, and Sana Alam. 2021. "Protests in the times of social media: A case of farmers' agitation." *DEF COVID-19 Ground Report Series*. https://www.defindia.org/wp-content/uploads/2021/05/Farmers-Protests-Report.pdf

Iyer, Kavitha. 2022. "Delhi riots: How BJP leaders created a powderkeg that led to 2020 Hindu-Muslim violence." *Article 14 Report*, October 11. https://article–14.com/post/delhi-riots-how-bjp-leaders-created-a-powderkeg-that-led-to-2020-hindu-muslim-violence-6344d8d280625

Jain, Shinzani. 2024. "India's farmers are mobilizing against the Modi Government." *Jacobin*, April 4. https://jacobin.com/2024/04/india-farmer-protest-modi-2024-elections/

Jaswal, Srishti. 2024. "Inside the BJP's WhatsApp Machine." *Pulitzer Center*, May 15. https://pulitzercenter.org/stories/inside-bjps-whatsapp-machine

Kaskar, Zeeshan. 2024. "India leads global internet shutdowns for sixth year straight: Report." *The Wire,* May 15. https://thewire.in/rights/india-leads-global-internet-shutdowns-for-sixth-year-straight-report

Kaul, Vitasta, and Vedaant Lakhera. "Delhi riots 2020: Five years on, trauma runs deep." *The Frontline*, March 18. https://frontline.thehindu.com/society/delhi-riots-2020-survivors-await-justice-compensation-five-years-later/article69344521.ece

Livemint. 2024. "Farmers protest: Centre blocks 177 social media accounts to maintain 'public order'." *Livemint*, February 20.

Mahapatra, Sangeeta and Johannes Plagemann 2019. "Polarisation and Politicisation: The social media strategies of Indian Political Parties." *GIGA Focus Asia*, 3, http://nbn-resolving.de/urn:nbn:de:0168-ssoar-61811-8

Mishra, Dibyendu, Syeda Zainab Akbar, Arshia Arya, Saloni Dash, Rynaa Grover, and Joyojeet Pal. 2021. "Rihanna versus Bollywood: Twitter influencers and the Indian farmers' protest." *arXiv* preprint arXiv: 2102.04031. https://joyojeet.people.si.umich.edu/RihannaVsBollywood

Mohan, Janani. 2021. "Media bias and democracy in India." *Stimson,* June 28. https://www.stimson.org/2021/media-bias-and-democracy-in-india/

Mohsina, Nazneen. 2020. "Hindutva vigilantism: Online hate, offline harms." *GNET – Global Network on Extremism and Technology*, October 22. https://gnet-research.org/2020/10/22/hindutva-vigilantism-online-hate-offline-harms/

Nair, Srishti. 2021. "India's struggle against fake news." *Institute for Internet & the Just Society,* February 7. https://www.internetjustsociety.org/indias-struggle-against-fakenews

Panijar, Tejasi, and Prateek Waghre. 2023. "IT amendment rules, 2023 are a nightmare, dressed like a fact checking daydream." *Internet Freedom Foundation.* https://internetfreedom.in/public-brief-it-amendment-rules-2023/

Poonam, Snigdha, and Samarth Bansal. 2019. "Misinformation is endangering India's election." *The Atlantic*, April 1.

Rajvanshi, Astha. 2024a. "2023 was the worst year for internet shutdowns globally, news report says." *TIME,* May 16. https://time.com/6978512/internet-shutdowns-india-report/

Rajvanshi, Astha. 2024b. "How Modi's supporters used social media to spread disinformation during the elections." *TIME*, June 3. https://time.com/6984947/india-election-disinformation-modi/

Ravi, P. 2021. "Shadow bans, criminal cases, takedowns: Inside India's expanding digital crackdown." *Article 14,* July 26. https://article–14.com/post/shadow-bans-criminal-cases-takedowns-inside-india-s-expanding-digital-crackdown-60fe1ebd5f3d0

Reporters Without Borders (RSF). 2020. "How India's government tries to suppress all COVID-19 reporting." April 4. https://rsf.org/en/how-india-s-government-tries-suppress-all-covid-19-reporting

Reporters Without Borders (RSF). 2023a. "India (down 11 at 161st)." In *2023 World Press Freedom Index – Journalism Threatened by Fake Content Industry*. RSF Report, May 3. https://rsf.org/en/2023-world-press-freedom-index-journalism-threatened-fake-content-industry

Reporters Without Borders (RSF). 2023b. "Modi ramps up online censorship in India," November 4. https://rsf.org/en/modi-ramps-online-censorship-india

Reuters. 2023. "India editors warn fake news proposal akin to censorship." *Reuters*, January 19.

Ruijgrok, Kris. 2021. "The authoritarian practice of issuing internet shutdowns in India: The Bharatiya Janata Party's direct and indirect responsibility." *Political Practice in Authoritarian Contexts (P-PAC) Blog*, University of Amsterdam, October7.https://ppac.blog/2021/10/07/the-authoritarian-practice-of-issuing-internet-shutdowns-in-india-the-bharatiya-janata-partys-direct-and-indirect-responsibility/

Singh, Manish. 2021. "Twitter restricts accounts in India to comply with government legal request." *Tech Crunch*. https://techcrunch.com/2021/06/07/twitter-restricts-accounts-in-india-to-comply-with-government-legal-request/

Tieri, Silvia, and Amit Ranjan. 2023. "Covid-19, communalism, and Islamophobia: India facing the disease." *Social Identities*, 29(1), 62–78. https://doi.org/10.1080/13504630.2023.2207460

Tiwari, P. 2021. "The 'Greta Thunberg's toolkit' scandal and rule of law in India." *Al Jazeera,* February 23. https://www.aljazeera.com/opinions/2021/2/23/greta-thunbergs-toolkit-exposes-indias-failing-institutions.

Twitter Safety. 2020. "Disclosing networks of state-linked information operations we've removed." *Twitter Safety Blog*, April 2. https://blog.twitter.com/en_us/topics/company/2020/disclosing-networks-of-state-linked-information-operations-we-ve-remo

Vasudeva, Feeza. 2025. "Political deification and religious populism in Modi's India." *Populism,* 8(1), 133–160. https://doi.org/10.1163/25888072-bja10073

The Wire. 2023. "The digital construction of Hindutva needs more attention." *The Wire*, August 4.

Yilmaz, Ihsan, and Raja M. Ali Saleem. 2022. *Hindutva Civilizational Populist BJP's Enforcement of Digital Authoritarianism in India*. Populism & Politics (P&P). European Center for Populism Studies (ECPS).

9

MEDIA AS A TOOL FOR STRENGTHENING AUTHORITARIAN AND POPULIST TENDENCIES IN CENTRAL EUROPEAN COUNTRIES

A Case Study of Hungary

Martin Solik and Jan Graf

Introduction

After the collapse of the Soviet Union and the great triumph of the Western bloc under the leadership of the US, it seemed that liberal democracy would in time replace the other types of political regimes that were present in the world at the time. In May 2004, when Malta, Cyprus, and the eight former Eastern Bloc states (post-communist and former Soviet republics) joined the European Union (EU), it seemed that the liberal democratic concept had indeed prevailed.

As part of this process, the EU required, among other things, that candidate countries adopt liberal standards and protect media independence. This requirement is set out in the Charter of Fundamental Rights of the EU in Article 11, point 1: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." and in point 2: The freedom and pluralism of the media shall be respected (Official Journal of the European Communities 2000). After Malta, Cyprus and eight post-communist countries met the challenging conditions and achieved full EU membership, a wave of enthusiasm swept through European society. Observers were optimistic and expressed hope that the new Member States would continue the process of democratisation and the development of civil rights.

However, after the initial enthusiasm for strengthening democratic principles and civil liberties, sobering sobriety set in. In recent years, a growing phenomenon of political transformation can be observed, especially in the Central European area. Populist, anti-liberal, and authoritarian tendencies

DOI: 10.4324/9781003628088-12
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

have been making significant inroads into the European political scene, sparking a general debate about the stability of democracy and the protection of liberal values. The well-known and famous split of opinion in the early 1990s between two erudite political scientists, the aforementioned Francis Fukuyama and Samuel Huntington, on the future of the world and the place of liberal democracy in real politics, respectively, has been rekindled.

There has been a sharp increase in populist political parties and movements, such as in Poland the Law and Justice Party; in Slovakia Direction: Slovak social democracy; in Czechia the ANO movement and Freedom and Direct Democracy; in Austria the Freedom Party of Austria; and last but not least in Hungary Fidesz (Hungarian Civic Alliance). Thus, the phenomenon of what has come to be called "democratic backsliding" is becoming more and more common.

According to the proponents of this concept, the quality of democracy, democratic values, and democratic institutions in different types of countries is gradually declining due to a combination of factors. If this process is not controlled, democratic decline causes a country to lose its democratic elements and become a country with a hybrid political regime or even an openly authoritarian regime.

In the case of Hungary, there are three major authoritarian tendencies that have the effect of weakening democratic values and civic aspects. The first is the curtailment of media freedom, with the Orbán government long criticised for its control over the public media and the restriction of independent journalistic institutions. A 2022 report by Reporters Without Borders ranked Hungary 85th out of 180 countries in terms of press freedom (Reporters Without Borders 2022). Ranking behind countries such as Serbia, Malawi, or Guinea demonstrates a stunning decline in this regard. Hungary's drop in the press freedom rankings came after 2010. In that year, Hungary was ranked 23rd out of 178 countries (Reporters Without Borders 2010).

The second example is the manipulation of the electoral system, which influences the political competition in favor of the ruling Fidesz. A comprehensive reform of the electoral system was a major issue for Fidesz after coming to power in 2010. While some minor changes were overturned by the Hungarian Constitutional Court in 2013, most of the components of the new electoral system came into force in 2012 and were reflected for the first time in the 2014 parliamentary elections. The reformed electoral system favors the big parties (favoring Fidesz) and weakens the smaller parties (a case of Hungary's disparate and fragmented opposition).

In Hungary, the independence of the judiciary is also being curtailed (in particular, the activities of the Constitutional Court have been curtailed). The Orbán government has implemented reforms which have led to an apparent link between politics and the judicial process. The Fidesz government also restricts the rights of activists and NGOs, which are often not allowed to

operate as in other democratic states. It is well known that the Orbán cabinet has long been opposed to George Soros, who is seen as the global face of third civil activism. It is Soros and his foundation that, following the example of Russia – where, in the context of legislative measures against NGOs, he has been negatively portrayed as undermining the sovereignty of states through the civil sector – is increasingly becoming a target of illiberal politicians and their supporters around the world (Solik and Baar 2019).

In June 2017, an almost identical law was adopted in the Hungarian Parliament to the one adopted earlier (in 2012) in Russia. Specifically, it was a law targeting foreign-funded NGOs. The law requires civil groups receiving foreign donations above a certain threshold to register as organisations funded from abroad. In this case, Orbán is aware that it is the NGOs, the nonprofits, that point to his political missteps and the overall limitations of democratic principles. Orbán's political discourse has also caused the polarisation of Hungarian society, in which the space for a pluralistic political contest is therefore limited.

This chapter focuses on the evolution of political transition and media freedom in Hungary, where Viktor Orbán has been in power since 2010 and since then a shift in political interests can be observed, especially in the context of state-controlled media. During the course of Viktor Orbán's rule, the politician has committed himself to rethinking the concept of liberal democracy in favor of a new political framework. The "illiberal era" was essentially inaugurated by Orbán's speech in the summer of 2014 in the Romanian town of Băile Tuşnad to members of his ruling Fidesz party. The speech was framed in the sense that "the era of liberal democracies is over" (Keating and Kaczmarska 2019).

This promoted political framework, which emphasises authoritarian elements, is of course also visible in the media sphere. Measures have been applied for a long time to control both free and state media, and political and economic pressure has led to a gradual loss of freedom in Hungarian journalism. The chapter therefore focuses on the transformation of the media sphere in Hungary and examines how pro-government media devalue (using sophisticated modern and digital tools) democratic and liberal values.

Information in this chapter is important contribution to understanding of how digital spaces are utilised to shape public opinion, particularly in regions like Central Europe. The overarching aim of this study is to shed light on the dynamic nature of Hungary's public and private media, with a specific emphasis on the driving forces behind these changes. The analysis reveals how state-run media are effectively used as tools to bolster authoritarian tendencies and erode democratic principles. The contribution, as in the other chapters, is based on SDIOs as a comprehensive framework that integrates various dimensions beyond the conventional military-political focus of IO.

Restrictions on media freedom can lead to violations of these rights and limit pluralistic views of society. In principle, since 2010, Fidesz has gradually shaped the media into a form that has become a propaganda tool. It only allows content that is in line with the ruling party. Although investigative journalism still exists in the country, the state news agency and the public media stop any journalist who wants to publish information about corruption cases linked to government officials. Thus, for Hungary's ruling elite, independent journalists are seen as "political actors" rather than individuals who gather important information for the public interest (O'Leary-Cyr 2022). The rights of sexual minorities in Hungary are a chapter in themselves. Orbán has a negative attitude toward the LGBT community, which of course translates not only into Hungary's anti-liberal policies but also into the society itself (Solik 2022).

It can be stated that the controlled destabilisation of public and private media in Hungary rests on three fundamental mechanisms: legislative measures, financial manipulation, and political pressure. One can undoubtedly agree with this definition, and the following pages will provide concrete examples of destabilisation through two of these three sophisticated mechanisms. Here, it is necessary to stress that these mechanisms meet the requirements of special, unconventional hybrid operations directly controlled by the Hungarian government. The Orbán system does not prohibit the operation of opposition media directly, by any explicit ban, but its ambition to make their existence impossible by economic (financial pressure), psychological, or legal means is unambiguous (Oktatói Hálózat 2020).

Destabilising Media Independence Through Three Mechanisms

The first mechanism that is used to destabilise the media is legislative measures. In the case of the destruction of the free press, or independent journalism, legislative measures and regulatory legislation appear to be the very tool that can be used to sophisticatedly prevent the functioning of free and private media. This can be done in two ways: "1) pursuing legislative action to determine media rights (and crimes) and, 2) using legislative action to bring state institutions and media regulatory bodies under partisan control" (Altena 2017).

In this regard, 2011 was a key year for Hungary. Since 2011 a comprehensive media law has been in force, which included the creation of the National Media and Infocommunications Authority (NMHH), which is involved in frequency allocation and control of compliance with the rules of the media law. The NMHH directly increased government control over print news, radio, and television and tightened regulations over public and private media sources in Hungary. Several authors analyze this type of mechanism in their contributions (see, e.g., Bajomi-Lázár 2013; Bajomi-Lázár 2014; Bayer,

Urbán and Polyák 2019; Gamboa 2022; Riaz and Rana 2024). That is why this chapter focuses on the remaining two types of mechanisms – financial manipulation and political pressure. These mechanisms have not yet been the subject of in-depth research.

Financial Pressure and Manipulation

In addition to the legislative measures aimed at consolidating the media space or, on the contrary, destabilising anti-government journalists, the ruling party uses another mechanism – financial manipulation – as a tool for deeper consolidation and centralisation of power over public and private media. It should be noted that financial manipulation can be part of complex legislative measures.

It can be said that this second mechanism is largely related to the financial and economic crisis of 2008. The great financial crisis of 2008 affected the whole world. In the European context, the Central and Eastern European region was affected to a much greater extent than the rest of the continent. Of course, the global financial crisis also had an impact on the media. As Václav Štětka presents, for the CEE region the crisis brought "another structural challenge to both media business and journalism in this region, namely the sharp decline in advertising resources" (Štětka 2013). Fewer financial resources available to the media after the 2008 economic crisis meant that media networks became particularly vulnerable to political influences. In this regard, not only Czech academics but also Péter Bajomi-Lázár suggest that, as a result of the lack of funding for the media after the global crisis, political parties and political actors were able to use this situation to their advantage and initiated (closer) financial ties with the media. In other words, after 2008, a substantial part of the media in Central and Eastern Europe aligned themselves with political parties that had monetary resources, and these media became increasingly dependent on political advertisements and government funding (Štětka 2013; Bajomi-Lázár 2013).

The destabilisation of the media through financial measures takes place specifically in Hungarian conditions through three channels.

(1) increasing costs for media outlets. The political actors, or rather the ruling political establishment, practice (through the relevant bodies, councils, and funds) financial manipulation and pressure by increasing the operating and licensing costs for selected media outlets, not only by increasing the expenditure on advertising taxes and licensing fees but also by imposing fines on media outlets that do not comply with the rules. While raising taxes and providing funding is not in itself illegal, it is a sophisticated tactic and a highly effective process. It is a tactic that, in principle, in line with legislative measures, does not financially support rebellious and

opposition (left-wing) media and, on the contrary, generously rewards pro-government media. In accordance with legislative measures, the ruling elite financially blocks or does not support rebellious opposition media and, on the contrary, generously rewards pro-government media. Higher taxes have made it costly for media outlets to oppose the ruling party or to sustain the voice of the opposition.

Within this first channel, it is essential to mention the Media Service Support and Asset Management Fund (MTVA). The MTVA was established on January 1, 2011, following a decision by the Hungarian government, which consolidated funding for public media under the Media Council's jurisdiction just through the MTVA. The MTVA would report to the Media Council and was responsible for financial and corporate decisions of Hungarian public media. This body decides on tenders for TV and radio broadcasting licenses and approves media mergers. As a result of this merger, three previous Hungarian public media institutions were deprived of their autonomy and financial decision-making: Hungarian Television (MTV), Hungarian Radio (Magyar Radio), and Danube Television (Duna Televizio) (Altena 2017). The Media Fund's Director is appointed by Chair of the Media Council.

In practice, this means that NMHH and the Media Council are in control of substantial financial resources. As presented by Bajomi-Lázár, by virtue of the 2011 Budget Act, the media authority had a budget of more than 29 billion forints (10,386,500 euros at the 2011 average exchange rate) for its own costs and the Media Fund a budget of over 63 billion forints (22,563,660 euros) to distribute; thus, the total sum Annamária Szalai (President of the NMHH in 2010–2013) ultimately controlled amounted to about 0.3% of the national GDP. The new regulation does not specify the Media Fund's allocation criteria. In addition, public service broadcasters outsource program production and advertising to companies close to the Fidesz party (Bajomi-Lázár 2013).

The Orbán government also undermines media plurality by making it more difficult for small media outlets to maintain the costs of operating independent outlets. Between 2010 and 2011, the Media Council doubled the costs of broadcasting licenses. In 2014, Fidesz also passed a new media tax to make it more burdensome for opposition media to stay in business (Altena 2017). In this respect, the Klubrádió radio case was a well-known example of how Orbán has limited opposition by increasing financial burdens on opposition outlets.

The commercial radio station Klubrádió, which is seen as the voice of the independent "anti-Orbán" left-wing opposition, lost its long battle with the government machine in February 2021 after the NMHH or the Media Council refused to renew Klubrádió's license for the frequency (92.9 MHz) on which it broadcasts. According to the NMHH, the radio has repeatedly violated the media law (including "illegal management"),

and therefore the license cannot be automatically renewed (International Press Institute 2021). After February 2021, the radio has therefore had to resort to internet-only broadcasting. The station, which is popular among left-wing Budapest intellectuals, has been struggling for more than a decade. After Orbán's rise to power, advertisers turned away from the station because of fears of government hostility, state-owned companies stopped advertising, and even lawsuits with regulators have not helped advertising sales.

Since 2010, the radio has lost 12 licenses for frequencies outside the capital and broadcasts only in the metropolis. Klubrádió reporters have been banned from government press conferences, and ministers have begun boycotting the radio. After international pressure, a successful campaign to save it, student support, and several lawsuits, the media outlet finally received a seven-year license in 2013 and avoided bankruptcy. Its income is mainly made up of financial donations from around a quarter of a million listeners (Harzer 2021). Again, it is clear that opposition media entities that criticise the Orbán government have extreme difficulty in obtaining or renewing a license. According to Mertek Media Monitor, a Hungarian non-governmental media monitoring organisation, between 2018 and 2021, the Media Council awarded 75% of all tenders to local radio stations that serve Fidesz's interests (Mérték 2021).

(2) manipulating the advertising terrain. Ruling political actors have practiced financial manipulation by exploiting relations between media outlets and political advertising. As one example, political actors have manipulated advertising contracts to shape editorial content and spread political messages. In exchange for secured advertising contracts and financial stability, political parties have encouraged journalists to echo partisan messages and to disseminate political reporting. Overall, media outlets' reliance on advertising contracts has allowed political actors to increase their influence over editorial content, to encourage self-censorship, and to influence public discourse (Altena 2017). In other words, while pro-government media outlets are subsidised or directly published by public budgets, opposition media outlets face harassment from the authorities and are prevented by the government from obtaining advertising. The advertising market is controlled by the Orbán oligarchs, and they decide which media outlets the advertising goes to. Private companies, including foreign ones, are being blackmailed by the government not to advertise to critical media. The aim of this policy is not only to silence independent media but also to put them in a situation where their owners are willing or forced to sell them cheaply to other interested parties with sufficient funds. And in Hungary today, these are only the state and oligarchs close to the government (Morvay 2016).

(3) concentrating media ownership into pro-Fidesz hands. The implications of media ownership concentration are that it is far more difficult for

> smaller, independent media outlets to compete with larger media moguls. In this case, Orbán has had wide opportunity to undermine independent media by consolidating media ownership into pro-Fidesz hands. In this context, the fate of the left-wing daily *Népszabadság* is a prime example. It has been active in Hungary since the 1956 revolution. The media outlet was very active, exposing corruption cases of the Hungarian government, pointing out the sophisticated and well-functioning model of kleptocracy in Hungary, and portraying members of the Fidesz leadership "as rich men without any scruples" (Morvay 2016).

In 2014, an Austrian company, Vienna Capital Partners (a private equity owned by the Austrian speculator Heinrich Pecina), purchased the well-known Left newspaper, *Népszabadság*. Prior to this sale, *Népszabadság* received no state funding and had been losing economic support for years because of Fidesz's financial pressures (Lendvai 2018). In 2016, the Austrian owners sold the newspaper back to its Hungarian domestic owners. The reason given was the newspaper's economic difficulties. However, Vienna Capital Partners did not sell the newspaper back to owners opposed to the ruling Fidesz but rather brokered a deal with Opimus Press, a media group owned by people linked to Fidesz. Soon after the deal with Opimus Press, *Népszabadság* was completely closed down (Zaccagnino 2021). The end of *Népszabadság* did not come as much of a surprise because of its investigative activities. The only question was why the end came so suddenly, and especially conspicuously. Fidesz could have changed the newspaper to its own image gradually and with less acclaim, as it had already done with other media. The desire to take revenge on unpleasant journalists and the need to show that influential people concentrated in Fidesz structures can afford to do anything with impunity probably played a role in this.

In the same year, 2016, Hungary's second largest commercial television channel TV2 was simultaneously bought by media entrepreneur and government commissioner Andy Vajna from a presumably non-repayable "loan" provided by a state-owned bank. TV2 has been an obedient tool of government propaganda ever since (Bajomi-Lázár 2018).

It is clear that Orbán's financial manipulation of Hungarian media has effectively pushed the character of the media content toward the pro-government right, because opposition and left media outlets have been unable to withstand Orbán's financial pressures.

Political Pressure

The third mechanism by which the pluralism and independence of the media environment can be undermined is political pressure. In the broadest sense, the term "political pressure" can be defined as "political actors manipulating ideological space for political or partisan benefit" (Altena 2017). If political

pressure asserts itself in the media environment, then it is clear that "the agents of the political field (politicians, the government, the state, political factions, and so on) attempt to use the media in order to broadcast their political agendas" (Goyanes, Vaz-Álvarez and Demeter 2021). In addition to pushing a political agenda, political pressure from ruling elites is typically used to define media content, build ideological support, manipulate media messages, denigrate, intimidate or ridicule regime opponents, or isolate opposition media (Polyák 2019).

Political pressure can be exerted on the media through several factors. Political actors undermine public discourse by publicly questioning the legitimacy of the media. These actors essentially delegitimise independent media by publicly denigrating the media for its investigative work. Ruling elites also undermine media pluralism by forcing or discouraging media actors from publishing certain types of (sensitive) public news. For example, the ruling elite may put pressure on the media to avoid reporting (in print or online) on "sensitive topics" (organised crime, corruption of ruling elites, environmental threats). The goal of this tactic is obvious. There is an ambition to undermine the independence of the media by pressuring it to report on sensitive and controversial topics in a biased and tendentious manner (in favor of the ruling political party). In addition, political actors practice political pressure when they encourage journalists to publish advertorials and kompromat – statements that reiterate pro-government messages or criticise political actors.

In Hungary, systematic political pressure has been exerted on the media essentially since Fidesz came to power in 2010 to disseminate pro-government content (propaganda). This pressure has been channeled through government-created regulatory bodies to destabilise or transform the anti-Fidesz media, influence media content, and, above all, establish a conservative-traditionalist course in the country. It is understandable that journalists in both private and, above all, public media were primarily exposed to this pressure. The rise of Fidesz and the preparation for a conservative revolution in the country required uncompromising and decisive measures. As Hungary's media laws changed after Orbán became prime minister in 2010, there was also a clear-out of staff in state media. Many senior executives and hundreds of staffers were removed, union representatives said. Several of those who lost their jobs say they believe they were fired because they had been critical of Orbán's Fidesz party. Many talented journalists could not withstand the pressure and resigned. Indeed, it became increasingly difficult to maintain editorial freedom. Bela Varadi was one of them. Varadi was an anchor on a state television news show, and he was the first member of Hungary's Roma minority to hold such a job. In an interview, he presented that he quit because he was "appalled at the new regime." He said that on many occasions the scripts he had written for the show were edited and changed before airing to make them more "more government-friendly." Edited and approved versions of the news items were changed as well (Dunai 2014).

He resigned in 2011 and moved to the UK. Cases like Varadi were, or still are, numerous in Hungary.

Human Rights Watch reports in a comprehensive report in February 2024 that after 2010, there have been many different forms of political pressure that have grossly undermined the freedom and plurality of opinion of journalists. These cases include:

(1) demanding of loyalty and obedience of public media employees to the ruling Fidesz by senior pro-government editors. A well-known case is that of Balazs Bende, foreign news editor at public service broadcaster M1, who instructed the newsroom staff in this way. In a leaked audio recording from a 2019 meeting, Balazs Bende, foreign news editor at public service broadcaster M1, can be heard telling staff that "this institution doesn't support the opposition coalition," and "we all work accordingly" and that "anyone who doesn't like it should resign" (Human Rights Watch 2024).
(2) Instructions or clear orders directly from the highest circles of the ruling party to journalists of public media on how to inform the public about sensitive topics. A March 2022 Direkt36 investigation shows leaked emails dating back to 2019 from the Prime Minister's chief of press Bertalan Havasi to the director of the Hungarian Telegraph Office, MTI, which is the state news agency part of the public service holding company. The emails instruct the MTI on a story and how to write and source it. According to the Direkt36 investigation, the leaked emails show how the government exercises influence over news by having journalists working for publicly funded MTI consult with the government before reporting on certain topics, while preventing reporting on other topics, leaving no room for editorial or journalistic freedom (Wirth 2022a, 2022b).
(3) Intense political and editorial interference in the work of journalists. Tamas Bodoky, editor-in-chief at Atlatszo, an independent investigative news site, recalled several incidents to Human Rights Watch when he was contacted by government officials or Fidesz politicians concerning stories he was working on coupled with requests for meetings. Several cases are recorded in this direction. Andras Rostovanyi, who formerly worked at the publicly funded state TV channel M1, mentioned that he received direct orders by email from his editor not to refer to Human Rights Watch and Amnesty in his reporting. Human Rights Watch received multiple emails from Rostovanyi from his time at M1 that show political and editorial interference in his and others' work.
(4) Guidelines for journalists on what stories to write, how to write them, and, at times, what terminology to use. Particularly during the refugee crisis in 2015, journalists in the public media were instructed not to use the term "refugee" in any case but had to use the term "migrant." The

aforementioned journalist Rostovanyi said that he similarly had to use the word "migrant" instead of "refugee" and was instructed not to use pictures of migrant children in his reporting (Human Rights Watch 2024).

(5) Denigration and marginalisation of unruly, usually left-wing journalists. This is a persistent, sophisticated, and long-term trend of coercion aimed at destabilising, silencing, or transforming left-wing journalists and activists and thus gaining control of the entire media spectrum in Hungary. In contrast, right-wing and Christian-conservative media enjoy considerable government support and operate on a sophisticated and centralised basis. November 2018 was a significant milestone in this respect. The concentration of ownership of (right-wing) media in Hungary has shifted fundamentally. A media conglomerate was created, a totally concentrated pro-government media empire called the Central European Press and Media Foundation (KESMA), into which oligarchs with close ties to Prime Minister Orbán have invested more than 470 media titles, including TV stations, radio stations, newspapers, and online media (roughly three-quarters of the private media market) (Sata and Karolewski 2023).

The creation of the centralised KESMA was primarily to unite the allied right-wing media under a single flag, strengthen their position, and make their funding more efficient (total centralisation will allow significantly fewer people to access funding and prevent further leakage of funds). This was intended to further cripple the left-wing media, or the left in general, which is basically disintegrating in Hungary. Without financial support from the state, without foreign owners, or without support from abroad, they can hardly sustain themselves. In addition to the poor financial support for the Hungarian left, there is persistent ostracism and demonisation by pro-government journalists and activists. This has resulted in the country's only independent newspaper, *Népszava*.

In Hungary, there has been a clear negative shift in the perception of media pluralism and independence since the Orbán government took office. The public and private media, which used to operate relatively freely, have gradually lost the hallmarks of objectivity and professionalism. They have come under the control of the state or oligarchic groups close to the Fidesz government. In the long term, there is pressure on journalists, self-censorship, the dissemination of pro-government content, and, consequently, a distortion of press freedom. While violence against journalists is rare, reporters have reported increased pressure to reiterate pro-government messages and to toe the party line at risk of heavy fines, job dismissal, or a potential lawsuit.

These developments in Hungary are part of a dangerous trend in the CEE region, where political leaders with illiberal tendencies often use their power to restrict media freedom and strengthen their political control. This tendency

is worrying for democracy and the rule of law in the region, and requires attention from both the international community and the citizens themselves who are fighting for freedom and democratic values (Šimunjak 2020).

One particular element of political pressure against the media that is being used by the Hungarian government is particularly dangerous and could have far-reaching consequences. This is the long-standing vilification and demonisation of left-wing journalists and activists in the country. Government politicians and the military and allied pro-government accredited journalists are publicly contributing to the distortion of the image of journalists who are ideologically and optionally different. They often portray them as frauds and actively conduct smear campaigns against them, branding them as traitors or public enemies. Verbal attacks on journalists using political narratives then become a common part of everyday political and social discourse. Unfortunately, this trend normalises hate speech against the latter group of journalists and allows it to become a common phenomenon in society (Stojarová 2020). Such attacks have serious consequences for the work of journalists and for the health of democracy.

Another key problem in the Hungarian media sphere is the issue of public media law. Although public media are formally labeled as "public," in practice they have become more like instruments of pro-government propaganda in Hungary. Although broadcasting regulation dictates that state broadcasting organisations must ensure pluralism of opinion, in reality the media do not have sufficient independence and space to present different views. Paradoxically, excessive funding of public service media can lead to their dependence on political power structures and limit their ability to perform their role as independent sources of information. Political influences can affect the content, selection of topics, and presentation of information to serve a particular political agenda or interest (Bajomi-Lázár 2017). The Hungarian case is significant in this respect because it shows that the problem may be not only underfunding but also overfunding.

Conclusion

The aim of this chapter was to examine the transformation of public and private media in Hungary. It focuses on identifying the main mechanisms influencing this transformation and, through media analysis, aims to show how state-controlled media serve as a tool to promote authoritarian tendencies and undermine democratic values.

This chapter shows how media transformations in Hungary are taking place and through which mechanisms the transformation is taking place. Basically, there are three key mechanisms through which media transformation takes place. The first key mechanism is the introduction of legislative measures. The most important legislative steps include the adoption of the

2010 law titled "Media and Press Freedom Act." This law made it mandatory for the media to provide fair, general, and balanced reporting. However, the law itself was heavily criticised by the European Union institutions, which considered it incompatible with democratic principles.

One of the main points of criticism was the powers given to the newly created media authority, whose members were appointed with close ties to the Fidesz party. This authority was charged with overseeing compliance with the rules laid down and had the power to impose significant financial penalties for breaches of the balance of coverage, effectively threatening the financial bankruptcy of the media. Fidesz used legislative measures to change the constitution and other laws, which had the effect of influencing the media space in favor of the ruling party. The establishment of institutions such as the NMHH (National Media és Hírközlési Hatóság) and the Media Council has strengthened control over the media while limiting independent and pluralistic media. In this way, Prime Minister Orbán has managed to centralise the media market, thereby strengthening the authority of the ruling political party and severely limiting the space for the existence of an independent press.

The second fundamental mechanism is the application of financial pressure and manipulation. This process shows how public funding is used to favor media close to the ruling party, while non-governmental media face frequent sanctions and financial difficulties. In this way, the independent media are weakened and then come under the control of new owners who support Viktor Orbán's political agenda. An example is the situation surrounding Klubrádió, which has not had its license renewed and now has to rely on financial donations to continue its operation. Another telling example is the case of the TV2 television station and the *Népszabadság* newspaper, which have been taken over by new owners who are close to Viktor Orbán's politics. This type of financial pressure and manipulation creates an imbalance in the media environment and limits the plurality of opinions and information available to the public. The consequence is the strengthening of the dominance of the pro-government media and the marginalisation of voices critical of the ruling party. This situation poses a serious threat to press freedom and democratic principles in Hungary.

The last important mechanism is political pressure. This chapter reveals various sophisticated forms of pressure, including the systematic discrediting and defamation of left-wing journalists and activists who are not in line with Viktor Orbán's political positions and ideology. These individuals are often the target of verbal attacks, which seriously threatens the free and independent work of journalists. Political pressure on journalists has been ongoing since 2010 and seems to have become even more intense in recent years. This pressure creates an unfavorable environment for the work of independent journalists and makes their professional activities much more difficult.

These three sophisticated mechanisms significantly destabilise not only opposition media but also the democratic way of developing the country. It is a complex and interconnected process. Opposition media are being questioned, with pro-government media deliberately questioning the legitimacy of these media outlets. In this way, the opposition media and its critical stance toward the government are devalued and marginalised, which ultimately creates a more serious problem – undermines media pluralism and disrupts democratic dialogue in society. The destabilisation of the opposition media and inconvenient politicians in Hungary through these three key mechanisms thus creates an elaborate and complex machinery that evidently pursues a higher goal – to gain dominant control over Hungarian society from the ruling Fidesz party. This consolidation of authoritarian elements and the undermining of democracy and pluralism is implemented through modern, specific measures that can be classified under the aforementioned broad-based SDIOs. All three mechanisms involve a range of subordinate manipulative measures (psychological operations, policy of deterrence, dissemination of disinformation, and dissemination of pro-government propaganda). They are thus part of the complex framework that is used in this publication. SDIOs are perceived as deliberate, technology-enabled efforts by state actors to manipulate the information environment, influencing both public opinion and collective emotions. This is exactly what the dominant Fidesz party (using various modern and digital tools) has been striving for in the long term – to gain total control over key segments of Hungarian society and break the remaining resistant politicians, journalists, and ordinary people too. This is essentially a state-controlled, complex hybrid operation against rebellious citizens, who have not yet identified with the authoritarian trend of the social-conservative Fidesz party.

State-controlled media, as in the case of Hungary, can be used to promote authoritarian tendencies by influencing news coverage in favor of the ruling party, suppressing criticism and silencing opposition voices. This undermines media pluralism and democratic control mechanisms, which can lead to restrictions on freedom of expression and citizens' access to independent information.

The consequence is also the discrediting of the opposition in the eyes of the public. By giving the ruling party an advantage in coverage and ignoring or downplaying the views of the opposition, the media build a mental barrier between "us" and "them." "We" are perceived as supporters of Viktor Orbán and the Fidesz party, who hold the right conservative views, considered to be the best for the future and development of Hungary. In contrast, "they" represent the "bad" opposition, often referred to in the media as representatives of Soros, a figure perceived negatively and pejoratively by a large part of the Hungarian population. In this way, the political polarised discourse is reinforced in an extreme way, and the portrayal of the opposition as enemies of the state's interests is promoted.

References

Altena, Hailey J. 2017. "Wrestling the Fourth Arm of Democracy: How the Orban Regime Undermined Media Independence in Hungary." M.A. Thesis, the University of North Carolina at Chapel Hill.

Bajomi-Lázár, Péter. 2013. "The Party Colonisation of the Media: The Case of Hungary." *East European Politics and Societies* 27(1): 69–89. https://doi.org/10.1177/0888325412465085.

Bajomi-Lázár, Péter. 2014. *Party Colonisation of the Media Central and Eastern Europe*. Budapest: Central European University Press.

Bajomi-Lázár, Péter. 2017. "Particularistic and Universalistic Media Policies: Inequalities in the Media in Hungary." *Javnost – The Public* 24(2): 162–172. https://doi.org/10.1080/13183222.2017.1288781.

Bajomi-Lázár, Peter. 2018. "Particularistic and Universalistic Media Policies: Inequalities in the Media in Hungary." In *Critical Perspectives on Media, Power and Change*, edited by Ilija Tomanić Trivundža, 129–139. New York: Routledge.

Bayer, Judit, Ágnes Urbán, and Gábor Polyák. 2019. *Media Law in Hungary. Alphen* aan den Rijn: Wolters Kluwer.

Dunai, Marton. 2014. "How Hungary's Government Shaped Public Media to Its Mould." *Reuters*, February 19. https://www.reuters.com/article/us-hungary-media-insight/how-hungarys-government-shaped-public-media-to-its-mould-idUSBREA1I08C20140219/.

Gamboa, Laura. 2022. *Resisting Backsliding: Opposition Strategies Against the Erosion of Democracy*. Cambridge: Cambridge University Press.

Goyanes, Manuel, Martín Vaz-Álvarez, and Márton Demeter. 2021. "Political Pressures in TVE: Cascade Effects, Morphology of Manipulations and Professional and Personal Reprisals." *Journalism Practice* 15(8): 1072–1088. https://doi.org/10.1080/17512786.2020.1772098.

Harzer, Filip. 2021. "Poslední neorbánovské rádio v Maďarsku je bez licence. 92,9 FM seodmlčí [The Last Neo-Orbán Radio Station in Hungary is Without a License. 92.9 FM Will Be Silent]." *Seznam Zprávy*, February 9. https://www.seznamzpravy.cz/clanek/posledni-neorbanovske-radio-v-madarsku-je-bez-licence-929-fm-se-odmlci–141492.

Human Rights Watch. 2024. "'I Can't Do My Job as a Journalist': The Systematic Undermining of Media Freedom in Hungary." *Human Rights Watch*, February 13. https://www.hrw.org/report/2024/02/13/i-cant-do-my-job-journalist/systematic-undermining-media-freedom-hungary.

IFLA. n.d. "The New Press and Media Act in Hungary." https://www.ifla.org/publications/the-new-press-and-media-act-in-hungary/ (Accessed February 1, 2024).

International Press Institute. 2021. "Hungary: Fidesz-Captured Media Regulator Blocks Latest Attempt by Klubrádió to Return to Airwaves." March 11. https://ipi.media/hungary-fidesz-captured-media-regulator-blocks-latest-attempt-by-klubradio-to-return-to-airwaves/.

Keating, Vincent C., and Katarzyna Kaczmarska. 2019. "Conservative Soft Power – Liberal Soft Power Bias and the 'hidden' Attraction of Russia." *Journal of International Relations and Development* 22(1): 1–27. https://doi.org/10.1057/s41268-017-0100-6.

Lendvai, Paul. 2018. *Orbán: Hungary's Strogman*. New York: Oxford University Press.

Mérték. 2021. "A Frekvenciapályázatok Háromnegyede a Fidesz érdekeit Szolgálja [Three-Quarters of the Frequency Tenders Serve the Interests of Fidesz]." October 29. https://mertek.eu/2021/10/29/a-frekvenciapalyazatok-haromnegyede-a-fidesz-erdekeit-szolgalja/.

Morvay, Peter. 2016. "Ako sa Népszabadság stal obeťou vládnej pomsty [How Népszabadság Became a Victim of Government Revenge]." *Denník N*, October 9. https://dennikn.sk/579008/ako-sa-nepszabadsag-stal-obetou-vladnej-pomsty/.

Official Journal of the European Communities. 2000. "Charter of Fundamental Rights of the European Union." December 18. https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Oktatói Hálózat 2020. "Hungary Turns Its Back on Europe: Dismantling Culture, Education, Science and the Media in Hungary 2010–2019." https://oktatoihalozat.hu/wp-content/uploads/2020/03/angol.pdf (Accessed December 12, 2023).

O'Leary-Cyr, Maya. 2022. "Press Freedom under Threat in Europe: A Case Study Analysis of The Increasing Threat to Press Freedom in Greece, Italy." Undergraduate Honors Thesis, The University of San Francisco.

Polyák, Gábor. 2019. "Media in Hungary: Three Pillars of an Illiberal Democracy." In *Public Service Broadcasting and Media Systems in Troubled European Democracies*, edited by Eva Połońska, 279–303. London: Palgrave Macmillan.

Reporters Without Borders. 2010. "World Press Freedom Index 2010." https://rsf.org/en/index?year=2010 (Accessed January 21, 2024).

Reporters Without Borders. 2022. "World Press Freedom Index 2022." https://rsf.org/en/index?year=2022 (Accessed January 21, 2024).

Riaz, Ali, and Md Sohel Rana. 2024. *How Autocrats Rise: Sequences of Democratic Backsliding*. Singapore: Springer Nature Singapore Pte Ltd.

Sata, Robert, and Ireneusz Pawel Karolewski. 2023. "Illiberal Spectatorship – The Disfigurement of Citizenship in Hungary and Poland." *Journal of Contemporary European Studies*. https://doi.org/10.1080/14782804.2023.2280977.

Solik, Martin. 2022. *Rusko a jeho pozícia globálneho neliberálneho lídra [Russia and its position as a global illiberal leader]*. Banská Bystrica: Belianum.

Solik, Martin, and Vladimir Baar. 2019. "The Russian Orthodox Church: An Effective Religious Instrument of Russia's 'Soft' Power Abroad. The Case Study of Moldova." *Acta Politologica* 11(3): 13–41. https://doi.org/10.14712/1803-8220/9_2019.

Stojarová, Věra. 2020. "Media in the Western Balkans: Who Controls the Past Controls the Future." *Southeast European and Black Sea Studies* 20(1): 161–181. https://doi.org/10.1080/14683857.2020.1702620.

Šimunjak, Maja. 2020. "Political Leaders, Media and Authoritarianism in Croatia: The Media Strikes Back?" *East European Politics* 36(1): 66–85. https://doi.org/10.1080/21599165.2019.1684267.

Štětka, Václav. 2013. *Media Ownership and Commercial Pressures. Final Report for the ERC-Funded Project Media and Democracy in Central and Eastern Europe*. Oxford: University of Oxford, Department of Politics and International Relations. https://www.academia.edu/8562331/Media_Ownership_and_Commercial_Pressures_Final_Report_for_the_ERC_funded_project_Media_and_Democracy_in_Central_and_Eastern_Europe

Wirth, Zsuzsanna. 2022a. "Leaked Documents Show How Orbán's Circle Dictates the News at Hungary's State News Agency." *Direkt36*, March 4. https://www.direkt36.hu/en/kiszivargott-iratok-mutatjak-hogyan-diktalnak-orbanek-a-nemzeti-hirugynoksegnek/.

Wirth, Zsuzsanna. 2022b. "'Please, Don't Report about this at all! Thanks!' – How the Hungarian State News Agency Censors Politically Unpleasant News." *Direkt36*, March 7. https://www.direkt36.hu/en/ne-ird-meg-semmilyen-formaban-koszi-igy-hallgatja-el-a-kormanynak-kinos-hireket-az-allami-hirugynokseg/.

Zaccagnino, Jessica N. 2021. "The Tragedy of Central European University: Theorizing Hungarian Illiberal Democracy and Its Threat to Academic Freedom." *Connecticut Law Review* 52(3): 1187–1242. https://digitalcommons.lib.uconn.edu/cgi/viewcontent.cgi?article=1451&context=law_review.

PART 4

Transnational Dynamics

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

10

IRANIAN STATE-SPONSORED DISINFORMATION AGAINST THE DISSIDENTS AT HOME AND IN THE DIASPORA

Shahram Akbarzadeh, Amin Naeni, Galib Bashirov, and Ihsan Yilmaz

Introduction

In September 2022, nationwide protests shook Iran following the arrest by morality police of Mahsa Jhina Amini and her subsequent death in custody. According to Iranian officials, this was "the most dangerous and powerful riot" against the ruling regime since 1979 (Khabar Online 2023). Despite the regime's successful use of force to quell street demonstrations, online activism emerged as a potent force. The 2022 protests invigorated anti-regime movements on social media to present an alternative narrative on power, politics, and accountability that challenged the official discourse. Since the 2000s, social media has afforded Iranians a platform to advocate for democracy, women's rights, economic prosperity, and international engagement, undermining the regime's narrative of popular loyalty to the highest Islamic jurisprudent, Vali Faqih (Golkar 2011).

Supreme Leader Ayatollah Ali Khamenei (2021) has expressed concerns about a "war of narratives" waged by external forces, particularly the US and its allies, to turn Iranian citizens against the regime. In response, authorities are actively restricting the internet, aiming to regain control over cyberspace and stifle dissenting voices. Beyond censorship, the Iranian regime has sought to spread online disinformation to subvert alternative narratives. Social media has emerged as a key battlefield between the state and society. Therefore, state-sponsored online disinformation campaigns have become a crucial tool for manipulating public opinion in Iran. This has led to the development of SDIOs under the Islamic Republic of Iran.

A key component of IO is the "Big Lie," a concept we use to denote a propaganda technique in which a series of sensational small lies forms

DOI: 10.4324/9781003628088-14
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

a cohesive and repeatedly asserted false narrative to distort reality across media platforms. This definition conceptualises the Big Lie as "pyramid" organised by "a configuration of smaller lies underneath" (Jacobson 2018). In the context of authoritarian regimes, the Big Lie is designed to present the official narrative as unquestionable truth. The Big Lie adopted in 2022/23 in Iran was a clear strategy to deny legitimacy to influential dissidents and prevent a potential alternative to the ruling regime. This Big Lie has relied on online technologies to reach a wide audience, specifically targeting tech-savvy opponents of the ruling regime.

In this context, this chapter examines the many components that serve as the foundation of the Big Lie, how they serve the ruling regime to set the political narrative about the future of Iran, and how the series of lies, untruths, and slanders feed into the idea that there is no better alternative to the Islamic regime in Iran.

Despite a wealth of research on online mis/disinformation (De Cock Buning 2018; Bradshaw & Howard 2018; Tsyrenzhapova & Woolley 2021), research on online Big Lies is rather underdeveloped. US President Donald Trump's Big Lie concerning the 2020 US Presidential Elections – which argued that the elections were stolen by the Democrats – has led to new interest in the concept (Kellner 2023; DiMaggio 2022). However, research is still underdeveloped in exploring how online Big Lies work in authoritarian contexts. Iran is an interesting case study where the theocratic authoritarian regime has attempted to construct a Big Lie in the face of an unprecedented existential challenge.

Iranian political system has attracted serious scrutiny, with the literature examining authoritarianism, corruption, and the crisis of political legitimacy (Parchami 2023; Kamrava 2022). The literature has also discussed various techniques the regime has used to control the internet, including widespread censorship and surveillance practices, and attempts to build an Iranian national internet in collaboration with China (Michaelsen 2018; Conduit 2022). This chapter contributes to this literature by exploring the specific ways in which the Iranian regime has utilised a key tool of disinformation: the Big Lie.

Using data from state-owned media content and pro-regime tweets, we discover that in the face of growing opposition and waning legitimacy, the Iranian regime has added a new approach to its arsenal of online IO. Originally, the Big Lie of the regime was that the US ("the enemy") was behind every opposition attempt in Iran. All dissent has been tarnished by associating it with a hidden US agenda. However, this Big Lie has lost its power of persuasion in the recent years as the Iranian public gains access to global news online. The idea that the US is to blame for everything that is wrong in Iran is now met with skepticism. In 2022, Iranian protesters vocally rejected that notion (BBC Persian 2022). Under such circumstances, the ruling regime

has sought to construct a new Big Lie to fortify its position. While the old Big Lie remains at play at the general level, particularly through traditional media such as television programs, the new Big Lie responds to new challenges in the wake of the popular movement that targeted the regime as a whole, and is adapted for digital propagation. It is designed to destroy the opposition's image online and devastate public hopes for an alternative to the Islamic Republic.

This chapter makes three interrelated contributions to the literature. First, it sheds light on the politics of the Big Lie, exploring the circumstances within which an authoritarian regime would devise a new Big Lie, specifically for an online audience. Second, it adds to the literature on digital authoritarianism by examining the learning capacity and adaptability of authoritarian rule in Iran. This study offers a new perspective on the significance of social media and cyberspace as new battlegrounds of ideas. And finally, it takes the discussion of the Big Lie away from the major cases of the US and Russia and demonstrates the relevance of the Big Lie concept to authoritarian regimes in the developing world.

To shed light on how the big lie emerged as a core strategy in state-sponsored disinformation campaigns, this chapter starts with a discussion of the Big Lie as a concept and its development in modern politics. Then, we explore the original Old Lie in the Iranian regime's propaganda and the development of the New Big Lie in recent years that reflects the ruling regime's adaptability to the changing political terrain. This is followed by a discussion on the rise of disinformation operations in modern authoritarianism and how the concept of the Big Lie can contribute to this discussion. After a brief section on the methodology, we move to the empirical section where we investigate the lies employed against three dissident groups. The overarching message that is delivered consistently is that the Islamic Republic is irreplaceable by opposition groups. The discussion in this section examines how the ruling regime has sought to discredit influential voices, thereby fostering a sense of hopelessness. The chapter concludes with a discussion of what the Iranian case reveals about the functions of Big Lies in modern authoritarianism.

Conceptual Framework: Big Lies in Modern Politics

The history of political rule is awash with lies told by politicians to deceive and conceal in order to rule with ease. Almost 500 years ago, Machiavelli suggested that "[t]hose princes who do great things have considered keeping their word of little account and have known how to beguile men's minds by shrewdness and cunning" (Machiavelli 1993, 221). The advent of radio and television in the 20th century gave way to a new, modern type of lying that is not only outlandish and colossal but also widely disseminated and repeated frequently. This dynamic led to the rise of what came to be known as "Big

Lies" that dominated the discourse of the 20th-century totalitarian regimes such as the Soviet Union and Nazi Germany.

The concept of the Big Lie is contested. The term has been applied to various claims in the 21st century, including the George W. Bush administration's assertion that Iraqi President Saddam Hussein possessed weapons of mass destruction (WMDs) and collaborated with al-Qaeda; Russian President Vladimir Putin's lie that Russian soldiers played no part in the annexation of Crimea in 2014; and Donald Trump's claim that the 2020 elections were stolen from him (Kellner 2023). The latter Big Lie was constructed on a series of smaller falsehoods, including claims of voting irregularities, corrupt officials, and manipulated voting machines. Trump's Big Lie and the following insurrection in the US Capitol have led to a renewed interest on the concept of the Big Lie (Kellner 2023; DiMaggio 2022).

Nonetheless, despite wide media coverage of Big Lies, conceptual discussion on the topic is scarce. The concept of the Big Lie remains poorly defined (Jacobson 2018; Bowler and Donovan 2024) and often does not go beyond a short, cursory definition (see DiMaggio 2022; Kellner 2023). There is consensus in the literature that the Big Lie rests on the operational premise that if you tell a lie loud enough, long enough, and with enough authority, people will begin to believe it (Cavanagh 2021). But what is a Big Lie? In asking this question, we recognise that a satisfactory definition of the term has not been provided in the literature. In a recent article, Edward Cavanagh argues that the Big Lie is "the strategy of subverting or even disregarding the truth in order to curry political favor" (2021, 69). While succinct, this definition leaves out some of the most important aspects of the concept, especially those pertaining to its content.

In a recent study, Lulat argues that "the Big Lie, which is usually a condensation of an outrageous conspiracy theory, is one of the foundational pillars of demagogic propaganda aimed at the masses" (2023, 112). This definition acknowledges the programmatic elements of the Big Lie even if the notion of "outrageous" remains ambiguous. Zienert-Eilts (2023) mentions two key features of the Big Lie which differentiate it from other forms of disinformation: that it is based on incessant repetition and that it distorts perceptions to a degree that it creates an "alternative reality" where the notion of truth itself is abandoned. We believe that presenting an "alternative reality" is a useful yardstick to distinguish a Big Lie. It will be difficult to reverse this alternative reality where "smaller lies help reinforce the credibility of the big lie and create a channel of facile manipulation" (Mishra & Jaramillo 2021).

This moves us to our definition, that a Big Lie is a propaganda technique in which a series of attention-grabbing small lies forms a cohesive and repeatedly asserted false narrative, distorting reality across media platforms. This definition helps make sense of historical and current Big Lies. As such, a Big Lie is an overarching narrative, not a single conspiracy theory or a falsehood

(DiMaggio 2022). For example, the Nazi Big Lie was that Germany lost WWI due to Jewish betrayal (Zienert-Eilts 2023). This message was a colossal lie as the reasons for Germany's defeat had nothing to do with Jews. But this statement also contains many false messages, conspiracy theories, and other forms of falsehoods. It included a series of small lies to shape and reinforce the Big Lie, including that Jews are secretly running the world, controlling foreign governments, and influencing German political life; Jews deliberately targeted Germany, besieged it, and wanted to destroy it. A Big Lie covers every aspect of social, political, and economic life and provides an alternative reality (Zienert-Eilts 2023).

A Big Lie needs to be constantly repeated in order to achieve the desired effect. In the 20th century, television and radio allowed dictators to propagate their lies to millions with ease. Thanks to their total control of the media terrain, they did not have to compete with alternative sources of information. In the 21st century, however, the rise of the internet and social media has complicated matters, as opposition groups use the internet to evade censorship. This has led authoritarian regimes to invest in cyberspace to spread propaganda and counter dissent.

The Big Lie in the Iranian Regime's Propaganda

In 1981, Ayatollah Ruhollah Khomeini, the founder of the Islamic Republic, declared that to save Islam, it is sometimes "obligatory to lie," emphasising that the Islamic regime (*Nezam*) is one of the foundations of Islamic principles, and its protection should be prioritised over other principles (Bastani 2018). Since the 1979 revolution, lying has become a tool through which the Iranian leadership attempts to impose a favorable narrative to gain legitimacy, deflect blame, and discredit its opponents (Bastani 2018). Central to this strategy has been the Big Lie that the US is behind every anti-regime activity. Since 1979, this message has been widely promoted by various high-ranking officials to manipulate public perception. For example, the Supreme Leader Khamenei has said that the US is "the enemy of the Iranian people," not merely the clerical establishment (Donya-e Eqtesad 2017). He has also characterised "America's enmity towards Iran" as "inherent" and "permanent" (Khamenei 2020). In Khomeini's words: "we have not experienced as much damage from any other source as we have from America" (Fars News Agency 2013). This anti-US narrative has advanced the regime's political agenda for many years and continues as an article of faith among the leadership. The official narrative aims to present the regime – which has been ruling with an iron fist for the past 45 years – as a victim and its opponents – who have been repressed at every opportunity – as tools of global oppression. When then-President Hassan Rouhani faced criticism in 2020, he said that critics should send their grievances to the right address: "the

White House" (IRNA 2020). In response to the 2022 protests, sparked by the death of Mahsa Amini, Supreme Leader Khamenei asserted that regardless of Amini's death, "I say frankly that these incidents were planned by the US, the Zionist regime and their followers" (Donya-e Eqtesad 2022). In fact, in his initial reaction to protests, he repeatedly emphasised the alleged involvement of the US, mentioning "America" 11 times and "enemy" nine times in a single speech (Donya-e Eqtesad 2022). Blaming the US as the overarching cause of all issues and Iran as the helpless victim has been the original Big Lie in the Islamic Republic of Iran.

However, there are signs that this Big Lie has lost credibility among the public; vocal voices in the country have challenged accusations that the US is the source of all problems in Iran. Since 2017, a poignant slogan has been trending in street protests: "Our enemy is right here; they [the regime] lie that it is America" (Iran International 2021). It has become increasingly challenging for the Iranian leadership to manipulate public perception with the tried and tired anti-US narrative. The regime's response to the 2022 protests marked the rise of a new Big Lie: the assertion that opposition groups are incapable of presenting a better alternative or shaping a brighter future. This is aimed at fostering public despair over the lack of viable alternatives, thereby making aspirations for change hopeless.

This new Big Lie has been promoted by state-owned and pro-regime media outlets, especially through their online accounts (Iran Newspaper 2022; Farhikhtegan Daily 2022). These propaganda activities have targeted influential dissidents with sensational lies, aiming to portray opposition figures as untrustworthy and to undermine hopes for a better alternative to the ruling regime. The old Big Lie was primarily propagated by high-ranking officials and traditional state media, such as television channels. The new Big Lie is predominantly disseminated in cyberspace with the assistance of mid-level officials, trolls, influencers, and various pro-regime social media accounts. This study will focus on the new Big Lie, exploring false narratives that have been constructed against opposition voices in social media.

Methodology

This chapter draws on online content spanning from November 2022 to November 2023. This was a pivotal period. The nationwide "Women, Life, Freedom" protests erupted in September 2022 and lasted for months. Dissidents made extensive use of online platforms to challenge the regime, share information, and organise impromptu rallies. The regime saw this as an existential threat, as the protestors chanted "down with dictator," an obvious reference to the Supreme Leader. The Woman, Life, Freedom movement was seen as an imminent threat to the continuity of the system which

required not only traditional responses of suppression but a robust response on the digital frontier. The ruling regime's new Big Lie was formulated and propagated online in this period. This study examines two types of Persian sources to shed light on how the regime targeted influential opponents in cyberspace.

First, stories published by state-affiliated online media are examined to show that they are the primary sources of lies in various cases. We have canvassed prominent Iranian news agencies such as *Fars News Agency*, *Tasnim News Agency*, *Hamshahri Online*, and the *Islamic Republic News Agency (IRNA)*. Starting from November 2022, these media outlets began a concerted effort to promote the idea that the opposition could not present a viable alternative to the Islamic Republic, stressing that the ruling regime is irreplaceable. This campaign focused on undermining the credibility of influential dissidents through character assassination and lies.

Second, in order to identify how narratives crafted by state-affiliated media have been disseminated to social media, we selected 163 posts on X (formerly Twitter). They were selected due to their connection to lies published by official media and their narratives in reinforcing pro-regime objectives at the expense of the opposition. Also, these tweets were specifically chosen for their publication within three days of the initial narratives crafted by official media. This defined time period helps detect the rise of coordinated waves of online campaigns. X was chosen as the focus for this research because it has become a key online battleground between opponents and supporters of the Iranian regime over the past decade (Kermani 2020).

Analyzing these two types of sources reveals how official and unofficial online agents of the regime have coordinated their efforts to portray influential dissidents as untrustworthy individuals.

The 2022 Protests: The Surge of Big Lies

Between 2009 and 2022, the Iranian regime encountered four nationwide protests challenging its rule. It is widely noted that the political legitimacy of the ruling regime is significantly challenged (Vakil 2022). The "Women, Life, Freedom" protests that unfolded in Iran in 2022 ignited a surge in state-sponsored disinformation on social media platforms. The resonance of these protests grew exponentially as advocates for the establishment of an effective alternative within opposition groups against the Islamic Republic took their message online. Against the backdrop of a deepening legitimacy crisis, the ruling regime intensified efforts to develop the Big Lie that there were no better alternatives for Iran. In a typical iteration of this Big Lie, the IRGC-owned Tasnim News Agency (2022a) argued that opposition groups would never provide an alternative because not only were they "corrupt" but also the Islamic Republic is based on "Iranian national and Islamic identity"

and the opposition could not offer anything better. State-owned Borna News Agency (2022) wrote:

> If not the Islamic Republic, who else will be? The monarchists? The People's Mujahedin Organization of Iran? The secularists? The secular democrats? The reformists? The pro-West and Pro-American agents? The ethnic groups? Which one of these can represent the entire Iranian people? Which one can build a better Iran? None of them. None of them accepts the leadership of another. And most importantly, none of them has a brilliant track record.

As such, the New Big Lie has targeted the credibility of influential dissidents, aiming to malign them as untrustworthy. Since 2022, the Big Lie propaganda has particularly focused on two primary groups. First, celebrities have found themselves increasingly in the crosshairs, as their influence over public opinion makes them potent figures in shaping alternative narratives. Second, prominent opponents in the diaspora have not been spared, as the regime seeks to disrupt their ability to present an alternative. In essence, key figures from these targeted groups are seen to represent a threat to the regime due to their capacity to influence public sentiment.

Celebrities

With the widespread use of social media, celebrities have garnered significant attention in Iran, often amassing over one million followers on Instagram. In exceptional cases, like that of Ali Karimi, the legendary Iranian footballer, the number of followers is around 15 million. This shows their capacity to influence citizens. In the 2022 protests, celebrities were very active in raising their voices against the Islamic Republic and showing their solidarity with protesters. At that time, Gholamhossein Mohseni Ejei, Iran's chief justice, warned that those who benefited from the system to build a career but aligned themselves with the enemy "must pay the price" (Hamshahri Online 2022). In January 2023, Iranian MPs announced that they would prepare a bill targeting "celebrities and popular figures" for "any comment in case of contradiction with the statements of the official authorities" (Hamshahri Online 2023). The IRGC-affiliated *Fars News Agency* noted, "A celebrity can cause more damage than a military person due to the connected network in society" (Fars News Agency 2022). While the popularity of celebrities has surged, state-sponsored Big Lie propaganda has attempted to discredit them. Their aim is to reinforce the Big Lie that opposition voices are incapable of forming a better future.

For example, a campaign was launched claiming that celebrities were urging people to protest as a means to qualify themselves for a US Green

Card (Jahan News 2022). This narrative was amplified on social media. In a tweet with more than 1,800 likes – a significant number in Persian tweets – a pro-regime user said sarcastically, "Celebrities say: Dear people of Iran, take to the streets and riot so that we can get visas, green cards, and asylum" (Yas 2022). Another user tried to mock celebrities and their followers, stating that "worthless people, celebrities, who sell themselves and their homeland for free with the promise of a green card; Worse than that, there are those who follow them" (Javadi 2022a). On the same theme, another user posted "celebrities are busy, completing their resume for a green card" (Yazdan-Parast 2022).

The celebrated footballer Ali Karimi became the target of a deliberate and sustained smear campaign. Karimi was vocal in his support of the protest movement to his large social media following. He is also wealthy with assets worth dozens of millions of US dollars. This factor played into the hands of the regime narrative when the majority of Iranians earn around $200 per month. A host of state-owned TV channels used a photoshopped image and claimed on Twitter: "Ali Karimi's US visa was granted, derived from the blood of the country's youth" (Sabeti 2022). This post received more than 7,700 likes and 1,300 retweets.

The photoshopped picture was disseminated by other pro-regime accounts. We found at least 43 tweets with the same picture and caption posted on December 15 and 16, 2022. They sought to propagate the narrative that Karimi supported "riots" to distinguish himself from Washington and gain a US visa, a clear strategy to tarnish his public standing.

Moreover, pro-regime accounts propagated the rumor that Karimi had sold his accounts on Instagram and X to Israeli intelligence services, Mossad, for US$2.5 million. We reviewed 40 tweets with the same message; similar keywords on Karimi were used between November 3 and 4, 2022. These posts received up to 2,500 likes, typically from accounts affiliated with the regime and its cyber warriors, indicating a coordinated campaign.

The second false narrative orchestrated by the Big Lie campaigns targeted women celebrities who appeared in public without wearing the mandatory hijab. They were labeled as mentally ill, a distorted characterisation crafted by the regime's judiciary system, a rare, if not unprecedented story with coordinated media coverage. At least two actresses, Afsaneh Baygan and Azadeh Samadi, who removed their hijab after the "Women, Life, Freedom" protests, were forced to undergo weekly psychological treatments for alleged mental illness (Etemad Online 2023). Their action in promoting a hijab-less lifestyle was perceived by the regime as symbolically encouraging other women to do so. This was a deliberate attempt to stigmatise these celebrities and discredit their message of defiance. State-affiliated newspaper *Hamshahri* covered the narrative on its front page with an article – titled "treatment of celebrity with a judge's prescription" – claiming that "bipolar disorder is the hidden illness of celebrities" (Hamshahri 2023). Subsequently, pro-regime accounts on X

started spreading the court's sentence for Bayegan and Samadi, emphasising that they had to go to see psychologists. For example, a user tweeted a photo of Samadi, saying that according to the court she has to take a psychological test every six months. His tweet, with four joy emojis, received more than 1,700 likes and 160 replies, mostly mocking Samadi (Nazi 2023). Another user highlighted that "The period of appeasement with celebrities who disturb the mental security of society is over. Details of the court's judgment for Afsaneh Bayegan [shows it], particularly the part that [she] should be referred to a psychologist once a week" (Barekati 2023). We noted 25 posts by accounts affiliated with the ruling regime between July 16 and 19, 2023, that attempted to propagate the narrative that Samadi and Bayegan present a threat to society due to their psychologically compromised state of mind.

This analysis reveals a concerted campaign to discredit celebrities, and an official stigmatisation of mental illness. In response, four Iranian psychology and psychiatry associations reacted by issuing a letter to the head of the judiciary. They described the sentences issued as "an abuse of psychology" and dismissed it as a common tactic in human history to subjugate political opponents. They provided examples, including the long-term Soviet imprisonment of dissidents in psychiatric hospitals, or the application of psychiatric diagnosis in the US history when dealing with rebellious slaves (Iran International 2023).

The aforementioned narratives illustrate the prominence of organised lying. The new Big Lie in the wake of the "Woman, Life, Freedom" movement rested on sustained and systematic dissemination of state propaganda in cyberspace. The origin of these lies can be traced back to the message in official media regarding the opposition's failure to present an alternative to the Islamic Republic. The campaign against celebrities who support anti-regime protestors was aimed at tarnishing their credibility and undermining their public standing. Portraying celebrities as opportunistic and mentally unstable made them look untrustworthy and their message of change delusional. All this was designed to kill hopes for change.

Prominent Dissidents in the Diaspora

The second group subjected to the Big Lie propaganda comprises prominent dissidents residing in the diaspora. The regime's strategy involves attempting to undermine their credibility by portraying them as morally or financially corrupt. This orchestrated effort aims to degrade and humiliate these individuals while concurrently disseminating a narrative that erodes public trust in their characters. For example, as the Pahlavi dynasty seems to regain a presence in the minds of Iranian citizens, the current ruling regime has escalated its attacks on its predecessor. The primary objective is to discredit Prince Reza Pahlavi, son of the late Mohamadreza Shah and a prominent symbol of

opposition to the ruling regime. On January 17, 2023, Ali Bahadori-Jahromi, the spokesperson of the Iranian regime, tweeted that the former Shah had taken national assets with him when leaving Iran in 1979. According to him, these included "two crowns containing 5,000 pieces of diamonds, 50 pieces of emeralds, and 368 pieces of pearls." His post received more than 2.6 million views, 7,200 likes, and 2,600 retweets (Bahadori-Jahromi 2023c). It was an obvious false story, as the two crowns are housed in the National Jewellery Museum in Tehran. A few days later, Iran's Minister of Cultural Heritage had to confirm that the two crowns are indeed in the Tehran Museum (Zarghami 2023). However, the purported tweet sparked a new wave of activity on social media among pro-regime accounts. We reviewed 68 tweets, posted between January 17 and 20, 2023, employing the hashtag "the Shah stole [Iran]" to target Reza Pahlavi. Pro-regime users attempted to propagate the idea that Reza Pahlavi should be held accountable for the assets allegedly "stolen" by Mohamadreza Shah.

Another target of the Big Lie was Nazanin Boniadi, a prominent human rights activist and actress extensively involved in advocating for the "Women, Life, Freedom" protests in the international community. In November 2022, when Boniadi attended a session at the United Nations and presented a case against the ruling regime in Iran, the official news agency, IRNA, published an article in which Boniadi was described with an offensive sexual label about her alleged relationship with Tom Cruise. The pejorative term may be translated into English as "sex toy of Tom Cruise" (IRNA 2022). The same story was published by *Tasnim News Agency* just two days later, and other state-controlled news websites also republished it (Tasnim News Agency 2022b). Simultaneously, the offensive slur was disseminated on X, with pro-regime cyber warriors posting content along the same line to discredit and humiliate Boniadi. We reviewed 30 tweets posted between November 3 and 6, 2022, that attempted to discredit Boniadi using the same offensive sexual narrative. They used the case of Boniadi to portray opponents to the Islamic Republic as corrupt, and lacking in dignity and morality. In this vein, Vahid Yamin-Pour, the then deputy of Iran's Ministry of Sports and Youth, tweeted, "The promotion of Nazanin Boniadi . . . is a testament to the long-standing desire of the West: The Iranian woman is considered alive and free only when she is a dancer and in the arms of foreigners" (Yamin-Pour 2022). His post received more than 4,400 likes and around 700 retweets.

The Iranian regime has employed attention-grabbing lies to undermine the credibility of dissidents in the diaspora. The regime systematically promotes the narrative that there is no viable alternative to the current state of affairs outside the borders of the country. It is part of the Big Lie propaganda that opposition figures are untrustworthy, and the Iranian people should not expect a better future with them. The ruling regime was clearly concerned about the message presented by dissidents and took measures to construct

and promote false narratives to discredit them and undermine public confidence in them.

The regime took advantage of social media, where lies can be spread easily. For instance, the tweets from the government's spokesperson on "stolen crowns," with over 2.6 million views, illustrate the capacity of social media in disseminating falsehoods. It should also be noted that posts on X receive likes, retweets, quotes, and mentions, creating a vast network for the Iranian regime to disseminate its narratives. Also, the Iranian leadership was aware that, due to a legitimacy crisis, traditional narratives should be replaced with character assassination and the humiliation of opponents. Therefore, the regime opted to employ the new Big Lie, attempting to humiliate prominent dissidents.

Conclusion

Since the 2022 "Women, Life, Freedom" protests, the ruling regime in Iran has intensified its disinformation campaigns to control the narrative. Since its establishment, the clerical regime has attempted to control the public by blaming the US for any anti-regime activity and domestic crisis. This narrative constituted the original Big Lie, propagated by high-ranking officials, typically in traditional media. However, this Big Lie has lost its traction as the public question the veracity of the anti-US narrative. Blaming the US for everything that is wrong in Iran is simply too convenient. A new Big Lie has emerged in this space, primarily in the digital sphere to bolster the regime's narrative in a time of crisis. State-affiliated online media and pro-regime accounts on social media have been the main propagators of the new Big Lie which seeks to convince the public that there is no better alternative to the Islamic regime by depicting opposition actors as corrupt and untrustworthy. The message being there is no future without the Islamic regime. To this end, the Iranian regime has leveraged state-affiliated media and pro-regime accounts on social media to advance its SDIOs. As highlighted in the first chapter of this book, SDIOs are conducted to provoke emotional responses and manipulate public sentiment in favor of political entities. In this context, the Iranian regime has crafted an online Big Lie to shape public opinion, using attention-grabbing false narratives to reinforce its digital strategy. To construct this Big Lie, the regime systematically disseminated a series of smaller falsehoods and distortions, gradually shaping a broader and more persuasive disinformation campaign.

The state utilisation of the Big Lie strategy rests on two primary reasons. First, there is compelling evidence that social media provides an environment conducive to the rapid and extensive dissemination of lies, outpacing the spread of truth. Second, the Islamic Republic has grappled with a significant legitimacy crisis, experiencing four nationwide anti-regime protests from

2009 to 2022. This has limited the regime's ability to maintain the facade of popular support. Instead, the regime has turned to systemic disinformation campaigns to discredit dissidents and undermine public hopes for an alternative. Aware of its inability to garner loyalty, the regime has attempted to spread hopelessness to ward off threats and enhance its chances of survival. A common pattern emerges within state-sponsored Big Lie campaigns against the three targeted groups. Humiliating opponents was seen as key for discrediting them. The new Big Lie, which combines conspiracy theories and slander, aims to portray influential opponents as opportunistic, corrupt, and self-serving. The ultimate objective of the Big Lie is to spread the belief that there is no alternative to the Islamic Republic, extinguishing hopes for a future without the ruling regime.

This case serves as a compelling example of how an authoritarian regime utilises digital technologies to navigate crises and ultimately enhance its chances of survival. This research also illustrates how modern authoritarianism works in a theocratic regime that has lost legitimacy among large segments of society. It shows that while there are similarities between the two, Big Lies differ from mere conspiracy theories or disinformation operations. While the latter are the staple of life in all political systems, including liberal democratic ones, the Big Lie is necessarily an authoritarian, if not a totalitarian, phenomenon. It is openly aimed at establishing and maintaining a dictatorship. The chapter also discussed how the internet has become a useful tool for authoritarian regimes to propagate Big Lies by flooding social media. The post-2022 developments in Iran have provided an apt case study.

Funding: This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.

References

Bahadori-Jahromi, Ali. [@alibahaadori]. 2023. "35 Billion Dollars of Iranian Property." *X (formerly Twitter)*, January 17. https://twitter.com/alibahaadori/status/1615031599137013760.

Barekati, Sobhan. [@sobhan_70]. 2023. "The Period of Appeasement with Celebrities Disturbing the Mental Security of the Society is Over." *X (formerly Twitter)*, July 19. https://twitter.com/sobhan_70/status/1681614060800843777.

Bastani, Hossein. 2018. "Lying for Saving Nezam." *BBC Persian*, December 18. https://www.bbc.com/persian/iran-features–46593800.

BBC Persian. 2022. "Iran's Foreign Minister: America has Told us Through Diplomatic Channels that it Does not Intend to Change the Regime." November 5. https://www.bbc.com/persian/articles/cx0yvg59yg0o.

Borna News Agency. 2022. "If There is No Islamic Republic." November 5. https://borna.news/005qyg.

Bowler, Shaun, and Todd Donovan. 2024. "Confidence in US Elections After the Big Lie." *Political Research Quarterly* 77 (1). https://doi.org/10.1177/10659129231206179.

Bradshaw, Samantha, and Philip N. Howard. 2018. "The Global Organization of Social Media Disinformation Campaigns." *Journal of International Affairs* 71 (1): 23–32. https://jia.sipa.columbia.edu/news/global-organization-social-media-disinformation-campaigns.

Cavanagh, D. Edward. 2021. "Countering the Big Lie: The Role of the Courts in the Post-Truth World." *Cornell Law Review* 72 (2). https://www.cornelllawreview.org/2022/06/26/countering-the-big-lie-the-role-of-the-courts-in-the-post%E2%80%91truth-world/.

Conduit, Dara. 2022. "Securing Iran in the Internet Age." In *The Palgrave Handbook of National Security*, edited by M. Clarke, A. Henschke, M. Sussex, and T. Legrand, 241–260. Springer International Publishing.

De Cock Buning. 2018. *A Multi-Dimensional Approach to Disinformation: Report of the Independent High-Level Group on Fake News and Online Disinformation*. Publications Office of the European Union.

DiMaggio, R. Anthony. 2022. "Conspiracy Theories and the Manufacture of Dissent: QAnon, the 'Big Lie,' Covid-19, and the Rise of Right-Wing Propaganda." *Critical Sociology* 48 (6): 1025–1048. https://doi.org/10.1177/08969205211073669.

Donya-e Eqtesad. 2017. "Leader of the Revolution: America Is the Enemy of the Iranian People, Not the Leader and the Government of the Islamic Republic." November 2. https://donya-e-eqtesad.com/fa/tiny/news–3308800.

Donya-e Eqtesad. 2022. "The Reaction of the Leader of the Revolution to the Death of Mahsa Amini and the Protests After That." October 3. https://donya-e-eqtesad.com/fa/tiny/news–3904725.

Etemad Online. 2023. "The Lawyer of Azadeh Samadi: The Judge has Published a Statement of Opinion in His Decision." July 16. https://www.etemadonline.com/tiny/news–622840.

Farhikhtegan Daily. 2022. "How Can the Events of 2022 Be Analysed? Movement or Riot?" December 6. https://farhikhtegandaily.com/news/76163/.

Fars News Agency. 2013. "America from Imam Khomeini's Worldview." October 3. https://farsnews.ir/news/13920711000773/.

Fars News Agency. 2022. "How Do Foreign Media Exploit Celebrities in Riots?" September 25. https://farsnews.ir/news/14020703000762/.

Golkar, Saeed. 2011. "Liberation or Suppression Technologies? The Internet, the Green Movement, and the Regime in Iran." *International Journal of Emerging Technologies and Society* 9 (1): 50–70.

Hamshahri Online. 2022. "Ejei's Warning to the Celebrities Who Became an Instrument of Enemies in the Riots." September 30. https://www.hamshahrionline.ir/news/709107.

Hamshahri Online. 2023. "Penalty Bill's Details for Celebrities' Comments." February 5. https://www.hamshahrionline.ir/news/739699/.

Iran International. 2021. "The Stock Market Losers Chanted the Slogan 'Our Enemy Is Here; They are Lying; It's America' During the Protest Rally." April 12. https://www.iranintl.com/20210412628999.

Iran International. 2023. "Warning of Mental Health Associations to the Judiciary; Psychiatric Abuse has an Unfortunate History." July 20. https://www.iranintl.com/202307202761.

Iran Newspaper. 2022. "Why is the Islamic Republic the Last Government of Iran?" November 12. https://ion.ir/news/7030.

IRNA. 2020. "Rouhani: The Address of All Crimes Against the Iranian People is the White House." September 26. https://www.irna.ir/news/84052431.

IRNA. 2022. "Defending the Rights of Iranian Women in the Style of a Sex Toy of a Hollywood Actress." November 3. https://www.irna.ir/news/84931917.

Jacobson, Zachary Jonathan. 2018. "Many are Worried About the Return of the 'Big Lie.' They're Worried About the Wrong Thing." *The Washington Post*, May 21. https://www.washingtonpost.com/news/made-by-history/wp/2018/05/21/many-are-worried-about-the-return-of-the-big-lie-theyre-worried-about-the-wrong-thing/.

Jahan News. 2022. "Gloriz: Celebrities Seek to Get Green Card." October 2. https://www.jahannews.com/news/813994.

Javadi, Ali. [@Alialialialyiy]. 2022. "Worthless People, Celebrities, Who Sell Themselves and Their Homeland for Free with the Promise of a Green Card." *X (formerly Twitter)*, October 5. https://twitter.com/alialialialyiy1/status/1577602615059300352.

Kamrava, Mehran. 2022. *Triumph and Despair: In Search of Iran's Islamic Republic*. Hurst Publishers.

Kellner, Douglas. 2023. "Alternative Facts, Political Lies, and Lying in Politics: A Paradigm of Bush and Trump Administrations." In *US Democracy in Danger: The American Political System Under Assault*, edited by A. Akande, 439–460. Cham: Springer Nature Switzerland.

Kermani, Hossein. 2020. "میدان سیاست در توئیتر فارسی؛ تحلیل کنشگری سیاسی همگان های شبکه ای در انتخابات جمهوری سال ۱۳۹۶ [Decoding Political Field on Persian Twitter: Analyzing Political Activism by Iranian Users During Iran's 2017 Presidential Election]." *Contemporary Political Studies* 11 (2): 149–186. https://politicalstudy.ihcs.ac.ir/article_5802.html.

Khabar Online. 2023. "Major General Salami: Last Year's Unrest was the Strongest and Most Dangerous Global Fight Against the Islamic Regime of Iran." August 1. https://www.khabaronline.ir/news/1796588.

Khamenei, Ali. 2020. "Remarks in a Meeting with People from Qom." January 8. https://farsi.khamenei.ir/speech-content?id=44628.

Khamenei, Ali. 2021. "War of Narratives, Today's Issue of the Media." *Personal Website of Khamenei*, December 12. https://farsi.khamenei.ir/others-dialog?id=49194.

Lulat, Y. G. 2023. "Trump's Big Lie and the January 6th Attack on the US Capitol: Going Beyond the Select Committee Report." In *The Perils of Populism: The End of the American Century?*, edited by A. Akande, 111–139. Cham: Springer Nature Switzerland.

Machiavelli, Niccolò. 1993. *The Prince (1513)*. Hertfordshire: Wordsworth Editions.

Michaelsen, Marcus. 2018. "Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran." *International Journal of Communication* 12: 3856–3876. https://ijoc.org/index.php/ijoc/article/download/8544/2462.

Mishra, Tanvi, and N. Jaramillo. 2021. "Exploring the Paradox of Why Colossal, Outlandish Lies Can Often Be Easier to Believe than Small Ones." *PROP Watch Project*, January 27. https://www.propwatch.org/article.php?id=275#5.

Nazi. [@Nazializadh]. 2023. "She Must Take a Psychological Test Every 6 Months." *X (formerly Twitter)*, July 16. https://twitter.com/Nazializadh/status/1680227619839565825.

Parchami, Aelius (Ali). 2023. "Neither Islamic, Nor a Republic and Not Iranian: The Legitimacy Crisis of the Clerical Regime." *Contemporary Politics* 30 (3): 316–340. https://doi.org/10.1080/13569775.2023.2283244.

Sabeti, Amir-Hossein. [@sabeti_twt]. 2022. "Ali Karimi's US Visa was Granted." *X (formerly Twitter)*, December 15. https://twitter.com/sabeti_twt/status/1603078727553933312.

Tasnim News Agency. 2022a. "From 'Berlin Conference' to 'Berlin Rally'; The Extension of the Helplessness of the Opposition Abroad." October 23. https://www.tasnimnews.com/fa/news/1401/08/01/2792489.

Tasnim News Agency. 2022b. "Get to Know Nazanin Boniadi More." November 5. https://www.tasnimnews.com/fa/news/1401/08/14/2798859.

Tsyrenzhapova, D., and S. C. Woolley. 2021. "Theories, Debates, and Innovation of the Russian Model." In *The Routledge Companion to Media Disinformation and Populism*, edited by Howard Tumber and Silvio Waisbord. New York, NY: Routledge.

Vakil, Sanam. 2022. "Iran's Crisis of Legitimacy." *Foreign Affairs*, September 28. https://www.foreignaffairs.com/middle-east/iran-crisis-legitimacy-mass-protests-ailing-leader.

Yamin-Pour, Vahid. [@yaminpour]. 2022. "The Iranian Woman is Alive and Free When the Dancer Is in the Arms of a Foreigner." *X (formerly Twitter)*, November 5. https://twitter.com/yaminpour/status/1588607035599622144.

Yas. [@s_yas_1]. 2022. "Dear People of Iran, Take to the Streets, Riot so that We Can Get Visas, Green Cards and Asylum." *X (formerly Twitter)*, October 12. https://twitter.com/s_yas_1/status/1579880577029005313.

Yazdan-Parast, Reza. [@yazdanparast313]. 2022. "Celebrities are Busy to Fill Out Their Resume for a Green Card." *X (formerly Twitter)*, October 3. https://twitter.com/yazdanparast313/status/1576863055589187585.

Zarghami, Ezatollah. [@Zarghami_ez]. 2023. "Today I Visited the Treasury #جواهرات_سلطنتی of the Central Bank." *X (formerly Twitter)*, January 25. https://twitter.com/Zarghami_ez/status/1617891104845869056.

Zienert-Eilts, Karin Johanna. 2023. "The Conspiracy Narrative 'The Big Lie' – Psychoanalytical Considerations on the Development of Susceptibility to an 'Alternative Reality'." *International Journal of Applied Psychoanalytic Studies* 21 (1). https://doi.org/10.1002/aps.1845.

11

THE INFLUENCE OF THE KREMLIN IN THE MEDIA SPACE OF WESTERN BALKAN COUNTRIES

A Case Study of Serbia

Jan Graf and Martin Solik

Introduction

In recent years, there has been an increased interest among analysts and academics in the issue of disinformation. Generally speaking, this interest has been triggered by the efforts of revisionist powers to change the distribution of power in the international system. It is in this sense that disinformation campaigns can serve as a tool that can be used for political purposes. A number of analysts point to the fact that, on a European and global scale, two revisionist powers in particular, Russia and China, are trying to create disinformation. However, different motivations prevail for the two states. While China is driven by the desire to improve its own image in front of the outside world (Speranza 2020), Moscow is taking a completely different approach. Moscow's goal in these situations is to destabilise the target states. By disseminating Russian narratives, the attitude of target societies toward key international political issues can also be changed quite well.

The issue of Russian disinformation campaigns has been addressed by a number of authors who mostly point to the Kremlin's efforts to overturn the results of elections and referendums. A striking example in this regard is the Brexit vote in 2016, when, with Russia's help, the people of the United Kingdom ultimately decided to leave the European Union. The Kremlin has also been accused of interfering in domestic political events in the case of the 2016 US presidential election, when Hilary Clinton and Donald Trump faced off. It was supposedly Moscow's efforts to create false information about the Democratic candidate that helped Donald Trump win that election (Walton 2019; Bjola & Manor 2021).

DOI: 10.4324/9781003628088-15
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

However, the desire to influence public opinion is also evident in continental Europe. How else to explain the fact that in 2023 only 58% of Slovaks surveyed fully supported their country's membership in the North Atlantic Alliance (Statista 2024)? It would be rather naive to believe that the current Russian leadership is not happy about such news. The Kremlin is trying to undermine the unity of the West and Euro-Atlantic integration structures through its narratives. A disunited West is weak in the eyes of the Russian political leadership, which may contribute to Moscow's rise to power. After all, the need to change the current alignment of forces in the international system, which the Kremlin believes, is dominated by the US and the West, can be found in a number of foreign policy concepts of the Russian Federation, which often include phrases about the need to strengthen Russia's position within the hierarchy of international relations (Foreign Policy Concept of the Russian Federation 2008, 2016, 2023).

The Western Balkans region is once again coming to the forefront of interest of world powers seeking to gain influence in these countries. On the one hand, the European Union (EU) and the US are trying to deepen economic and political cooperation with the Western Balkan countries. However, Russia and China are also seeking to extend their influence, and have recently been trying vehemently to change the balance of power within the international system. It is the Western Balkans that is thus finding itself at an imaginary geopolitical crossroads. It is becoming an area where the divergent interests of the key geopolitical players clash. The position of the Western Balkan states is becoming particularly important at this turbulent time, when the Kremlin, through its imperial policy, is trying to promote its own power interests by military means at the expense of its neighbor, Ukraine.

Russia's invasion of Ukraine in February 2022 certainly changed the situation in this respect. This military aggression against a neighboring country has led to a much greater degree of cooperation between the various European states, but more importantly, it is also beginning to manifest itself more and more strongly in political reality. It is important to realise that the very imperial mindset of the current Russian leadership is a strong impetus for the security architecture in Europe to begin to change. A number of states on the European continent have begun to increase their defense spending, and there has also been an expansion of the North Atlantic Alliance to include Finland and Sweden, which were previously militarily neutral states. However, the changing security situation on the European continent has forced both states to change their stance on this foreign policy issue. Moreover, for the Kremlin, the question of the expansion of the North Atlantic Alliance is a very pressing issue, and Kremlin leaders draw attention to this in their statements on a fairly regular basis. However, the Western Balkans remain a region that, with the exception of Montenegro, is not integrated into NATO, which is understandably attractive to Moscow.

Even from this perspective, the question of power competition over the Western Balkan states is a highly topical issue, which this chapter will try to look at through the element of Russian disinformation campaigns. Indeed, as already suggested in the introduction, these can contribute to destabilising the target states and, in turn, to strengthening the influence of the Russian Federation. This chapter will attempt to demonstrate this through the example of Serbia, where the environment is most conducive to the dissemination of Russian narratives. This is due, among other things, to the fact that Serbian society has long been in favor of cooperation with Russia. This can be demonstrated, among other things, by the fact that the only pro-Russian demonstration took place in Belgrade after Moscow attacked Kyiv in February 2022. The aim of this chapter is therefore to hit the most significant Kremlin narratives recently appearing in the Serbian media space, to point out the different Russian tools used to spread these pieces of disinformation and, last but not least, to show how the current Serbian political leadership is dealing with these narratives.

Disinformation and Its Conceptual Anchoring

Before presenting the most important Russian narratives in the Serbian media environment, it is certainly appropriate to clarify what disinformation actually is. At this point, it should be emphasised that this is not a new phenomenon, as disinformation has been spread in the world since the times of the most ancient civilisations (Kapantai et al. 2021). What has changed, however, and this was hinted at in the introduction to this chapter, is both the speed at which disinformation can be spread in the contemporary world and the number of people who can be affected by such disinformation. Indeed, globalisation has made it much easier to disseminate new information, making it known to a much wider range of people than was the case in the past.

As it is well documented in recent events, disinformation is gaining ground. It is not just about influencing election and referendum results, as in the case of the US presidential election or the referendum on the Brexit. Disinformation also played a role in the global pandemic COVID-19, where it often led to unnecessary deaths. Disinformation can have a number of negative effects on the target society, as shown by a number of papers already published on the subject. Among the most important ones are clearly the ability of disinformation to polarise society in terms of opinion (a phenomenon that appears especially in the online environment) (Törnberg 2018), as well as its ability to deepen distrust in the existing political representation (Balmas 2014; Littau & Stewart 2015) and, last but not least, to undermine trust in traditional media (Balmas 2014; Littau & Stewart 2015). These are all problems that disinformation can bring with it, and therefore it is important to study it systematically and in detail.

The prevailing view in academia is that there is no single definition of disinformation (Tambini 2020; Hoboken et al. 2019), despite the fact that authors try to name false or not entirely true information and half-truths in different ways. Different authors use labels such as "fake news," "false news" (Vosoughi et al. 2018), "digital misinformation" (World Economic Forum 2018) or more simply, some analysts use the term "disinformation" (Wardle & Derakshan 2017; Amazeen & Bucy 2019). Either way, analysts and academics essentially agree that the essence of disinformation is to present a fact intentionally or unintentionally distorted, which then implies the consequences that the recipient of such information carries with it.

The rise of disinformation and the efforts to eliminate it in the public space have brought with them the necessity to find an operational definition of this term, which is not only used by analysts of international relations but also commonly encountered through the media and commonly used by people in their everyday lives. Therefore, a number of analysts have attempted to define this very concept. This effort has also manifested itself at the institutional level. In a European Commission document, disinformation can be understood as "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit" (HLEG 2018), which is essentially the same as the definition provided by the Merriam-Webster Dictionary. This online dictionary defines disinformation as "false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth" (Merriam-Webster Dictionary 2024).

However, the authors Wardle and Derakshan (2017, 20) look at the whole issue from a different perspective, distinguishing between misinformation and disinformation. Both of these terms describe false information, but their harmfulness differs depending on whether or not they cause harm to the recipient of such piece of information. If such information causes harm to someone, it is disinformation. If it does not, it is misinformation. However, the previous definitions have one thing in common. They denote false information that is intentionally or unintentionally spread among people by some actor.

In the context of disinformation, Durach et al. (2020) note two significant features that they believe complicate the fight against disinformation. First, previous efforts to examine disinformation have not taken into account how people behave in the current online world but have focused mainly on individual phenomena (elections) and actors trying to influence public opinion (e.g., Russia). The second shortcoming then, according to these authors, stems from a lack of understanding of how the current online space works, as the emphasis is on traditional media to be the pillar in the fight against disinformation and to help people recognise individual untruths. This takes

no account of the advent of artificial intelligence and algorithms, which have transformed the whole online environment to a large extent. It is precisely these shortcomings that can then be exploited by individual actors to not only present their own views but also try to change other people's views as they see fit.

The whole empirical part is based on the concept of SDIOs, which were introduced in the introductory chapter of the book. The aim of this chapter is to explain how the Kremlin is trying to destabilise Serbian society through these operations.

Russian Disinformation Campaigns in the Western Balkans: The Case of Serbia

A number of manuscripts that address the issue of Russian disinformation campaigns note how the Kremlin uses its online media, as well as television stations such as Russia Today and Sputnik News (Giles 2016; Karlsen 2019). However, as Myhre et al. (2024) point out, most authors take it for granted that Russian disinformation campaigns have the potential to influence public opinion independently of the target society. According to these authors, however, this may not be entirely true, as one does not necessarily have to be influenced by Russian narratives in the media to adopt pro-Russian positions on key international political issues. It may just be a personal choice that a person makes, which may be conditioned by the relationship of several factors that should be examined more closely.

Russian disinformation campaigns in the Western Balkans have been covered by a number of authors in the recent past. Doncheva (2020) examined the narratives used by the Russian-based media outlet Sputnik Srbija and the effects these narratives have on the target societies. An important contribution to this discussion is the analysis of Metodieva (2019), which focuses on the specific media through which disinformation is presented to target societies. In this context, we cannot leave out the analysis of Duffy and Green (2020), who again focus their attention on Russian narratives in the Western Balkan region. Valuable data in this regard are provided by CRTA's analyses (2022a, 2022b; Kleut 2022), which focus specifically on the Serbian media space and reveal which Serbian media outlets adopt Russian narratives quite uncritically. Regarding Russian disinformation campaigns in Serbia, an interesting contribution is the analysis of Zivotic and Obradovic, who put Russian disinformation in context with the way hybrid warfare[1] is waged (Zivotic & Obradovic 2022).

In the case of Russian disinformation campaigns in Serbia, this chapter will focus on the specific ways in which pro-Russian narratives are promoted in the Serbian media space, with a particular focus on the content of Russian disinformation and the impact of current events in Ukraine on its content.

In other words, the following pages will discuss how the content of Russian disinformation has changed after Russia launched a full-scale invasion of Ukrainian territory in February 2022. Indeed, this event not only did bring about an imaginary break in the practice of defense policies of European states but was also reflected in the media space, as Wenzel et al. (2024) point out using the examples of the Czech Republic, Poland, and Slovakia. In their study, the aforementioned authors managed to highlight the main features of the Russian disinformation strategy in these states in the context of the ongoing conflict in Ukraine and describe what the main themes of this disinformation are.

As far as the Serbian media space is concerned, it is worth noting that it faces a number of problems, despite the Serbian government's efforts to make the Serbian media space transparent through reforms. Although these reforms started in 2014, they have not led to the expected results. Due to the lack of reforms, the Serbian government has faced numerous criticisms, especially from the EU, on the grounds that for the EU, this agenda is linked to freedom of speech, and if Serbia did not respect this value, it would not be able to join the Union because it would be out of step with the value framework of the entire Union (Bajic & Zweers 2020).

As numerous analyses by Media Ownership Monitor have pointed out, the media space in Serbia faces a number of long-standing problems. Their latest report, published in November 2023, says, among other things, "Problems include threats and negative campaigns against independent media and journalists, weak institutions and regulatory systems for protection, lack of transparency in media ownership and financing, favouring of pro-government media in the market, and state control over sources of funding" (Media Ownership Monitor 2024). In other words, it is the Serbian government that determines the amount of money to be given to independent media, which has been pointed out, among other things, in a negative sense by the European Commission, which has long criticised Belgrade for this attitude toward independent media (European Commission 2022, 2023). The global pandemic COVID-19 also contributed to this situation, with the Serbian government going after media outlets that were critical of its top officials. The Serbian government financially supported only pro-government media at this time (Cendic & Gosztonyi 2020).

Similar conclusions to the online Media Ownership Monitor website are also reached by the European Commission, which in its annual report assesses how Serbia is dealing with the implementation of the legislation required for EU accession. The organisation also concludes in its report that Serbia's reforms within the media space are insufficient, and that Serbia has made very little progress in this respect (European Commission 2023). The link between the political representation and the media remains a problem that Serbia should address.

Moreover, in October 2023, the Serbian parliament adopted a rather controversial amendment to the law, according to which the state can start buying media outlets again (Media Ownership Monitor 2023), which was not possible until then. It is these steps that lead to media outlets being controlled directly by either government structures or organisations that are pro-government. It is the media's dependence on the state apparatus that is often the target of criticism by independent institutions such as Reporters without Borders, which draws attention to the fact that independent journalists in Serbia are very often under pressure from government structures and are also forced to face indiscriminate attacks precisely from the government. Moreover, critical voices do not even have the right to ask unpleasant questions of government officials. In addition to these circumstances, this organisation notes that media outlets that are uncritical of the ruling SNS party are becoming an extended arm of the Kremlin as they uncritically adopt Russian narratives into their reporting (Reporters Without Borders 2023a, 2023b).

The connection between Serbian journalism and politics is also pointed out by Djuric (2022), who points out that there are many topics that cannot be covered by independent media because the ruling structures do not like it. Only topics that are not related to politics or that do not speak negatively about the representatives of the Serbian government can be discussed. After all, the excessive relationship between Serbian politics and journalists is also criticised by the European Commission (European Commission 2022).

The most striking example of the Serbian media's links with government officials is Telekom Srbija, which is directly linked to the Serbian government structures that de facto control it. Telekom Srbija controls more than 53% of the media market (RATEL 2023, 14). The second largest media company in the Serbian market is Serbia Broadband with a share of 40.5% (RATEL 2023), owned by the company United Group. The monopolisation of the Serbian media market also remains a major problem,[2] although laws have been passed to restrict this type of competition. In practice, however, these laws do not work well. While there are other laws in the pipeline that should further help to address the situation, the political will to enforce them is still lacking (Milutinovic et al. 2023). The whole situation is much more complex than it might seem at first glance, because it is not as if the entire media space is only dominated by pro-government media. In fact, there are also media in Serbia that are more in favor of the opposition. These are two television stations in particular – N1 and Nova (Milutinovic et al. 2023).

All these problems, which have been briefly described in the previous lines, may in some way contribute to the fact that Russian disinformation campaigns and narratives are so successful. However, the structure of the media and the shape of the media space in Serbia are not the only reasons why Russia is widely perceived as a Slavic friend and an important foreign policy partner, at least by Serbian society itself. The very shape of the media space

only serves to make it easier to reach potential audiences. What is important, then, is the Serbian political representation itself, whose actions feed these pro-Russian narratives. In this case, a crucial role is played by Serbian President Vucic himself, who almost to the day, exactly two years after the start of the Russian invasion of Ukraine, expressed his belief that there were friendly relations between the two nations (TASS 2024). In making his statement, the Serbian President referred to the pragmatic policy of his state. Even before the invasion, Vucic let it be known that 85% of Serbian society would be sympathetic to Russia, regardless of the Kremlin's policies on the international stage (TASS 2022).

Russia's disinformation strategy toward Serbia is based on two media pillars. These are RT Balkan (formerly Russia Today) and Sputnik Serbia. The latter is already operating in the country, as it has been since 2014, when its radio station was opened (Secrieru 2019). It is these two Russian media outlets that have the highest reach across the region. On the other hand, let us not overestimate their influence, because as will become clear from the following content of the chapter, the Serbian pro-government media are also responsible for spreading pro-Russian narratives.

The inclination toward Russia is mainly due to two reasons. First, it is due to the fact that Russia, through its own and Serbian pro-government media, effectively spreads anti-Western narratives, which is then reflected in opinion polls. The second significant factor is that Russia is positioning itself as a possible alternative to the democratic West, which it is constantly attacking rhetorically. The pervasiveness of Russian narratives is also highlighted in the European Commission's report (European Commission 2023). The report literally states that "Serbia needs to take urgent action to counter anti-EU narratives propagated by numerous media outlets, and to counter foreign information manipulation and interference, most notably in the context of Russia's war of aggression against Ukraine" (European Commission 2023, 6).

This inclination toward Russia is also clearly evident in surveys conducted by organisations that have looked at how people from outside the EU perceive the current Russia–Ukraine conflict. Vuksanovic et al. (2022a, 2022b), based on their data analysis, conclude that Serbian society is out of step with the rest of the societies of the countries surveyed. Sixty-three percent of Serbs surveyed concluded that the West is responsible for the current conflict in Ukraine. This opinion was held by the majority of the people interviewed only in Senegal, where 52% of respondents agreed with this idea. In the light of these data, it is not surprising that more than a third of the respondents (namely 35%) believe that Ukraine should not demand the return of the territories annexed by the Russian Federation. Only 12% of respondents then conclude that Russian military forces should not continue to occupy Ukrainian territory (Vuksanovic et al. 2022a). It is worth recalling at this point that

annexation is an act in flagrant violation of international law and that the international community does not recognise the annexed parts of Ukrainian territory as a legitimate part of Russian territory.

There are several reasons why the Serbian political representation also supports Russia and why relations between Belgrade and Moscow can be described as good even in the current turbulent times. The most important factor shaping the shape of relations between Serbia and Moscow is undoubtedly the unresolved issue of Kosovo's future territorial status. It is this dispute between Belgrade and Pristina that has long-led Serbian government officials to side with the Kremlin. In this case, Moscow has the potential to block any resolutions concerning this particular state. The pro-Serbian stance on Kosovo makes Russia a valuable ally for Belgrade, as it is the most pressing foreign policy issue for the Serbs.

The fact that the rhetoric of the Russian media in Serbia has always been tuned against the West and NATO is evidenced by the analysis of Tihomira Doncheva (2020), who in her 2020 analysis points out the main themes of the Russian disinformation campaign in Serbia using the example of Sputnik Srbija, one of the most influential media in this respect in this country. It should be added at this point that Doncheva analyzed over 2,000 articles published on this media outlet during 2018. Based on this thorough analysis, Doncheva was able to point out a number of narratives. First of all, the good relationship between Belgrade and Moscow was emphasised, and, on the contrary, the West was accused of expanding its influence in the whole region of the Western Balkans through this medium. There were also references to NATO being an aggressive and provocative organisation, or to member states treating the Western Balkan countries (Serbia) as their colony, which they exploit in this way (Doncheva 2020).

Of course, these reports can change people's attitudes toward EU membership. In 2020, only 26% considered Serbia's possible EU membership to be economically advantageous, while almost a quarter of respondents rated the country's possible EU accession as economically disadvantageous (Balkan Barometer 2020). These data directly correspond to two factors already discussed in this chapter. First, it is the loss of enthusiasm for the country's possible rapid integration into the EU and second, the negative media image of the Union causes the possible EU accession to lose support among Serbian citizens. This is not only due, first, to the media adopting the Russian narrative but also due to the Serbian political representation, which is unable to bring the country closer to EU membership through reforms. Serbian President Vucic's inclination toward Russia also plays a part in this.

As CRTA points out in its analysis (2022a), Vucic did not speak negatively about the Kremlin in his media appearances, even at the time when Moscow attacked Kyiv. Other government officials behaved similarly. They have quite often downplayed the whole situation in Ukraine and have long

avoided condemning Russian aggression at the UN. Although this eventually happened, Serbia did not impose sanctions on Russia for this criminal act (Knezevic 2022). According to the authors of this chapter, this is mainly due to a certain pragmatism of the current president Vucic, who is aware that Moscow is Belgrade's most vocal supporter on the Kosovo issue. Moreover, it should be borne in mind that any support for sanctions against Russia could lead to a decline in its popularity.

In June 2023, Aleksandra Godfroid, a Serbian journalist, expressed the opinion that the Serbian population tends toward Russia mainly because they see it as their protector, which is due, among other things, to the fact that Russia is seen as a state that has a fraternal and therefore friendly relationship with Serbia (Godfroid 2023). It is also important to mention, according to this journalist, that Russia tries to denigrate the West and Euro-Atlantic integration structures with its disinformation, which appeals to a certain part of Serbian society. An important element that Moscow uses in its rhetoric is Pan-Slavism. Russia's top officials very often refer to the fact that there is a bond between Serbia and Russia formed by the Orthodox religion.

The fact that media outlets linked to government officials are uncritical of the Kremlin in the Russian–Ukrainian conflict undoubtedly plays a role in the pro-Russian attitudes of Serbian society and government. As Kisic (2022) points out in his analysis, the vast majority of the pro-government media have, from the very first days of the Russian aggression, taken the Kremlin's side quite uncritically, as evidenced, among other things, by the headlines of the main Serbian media used in this analysis. It was the Serbian media that at the time mostly reported on Russia in positive or neutral terms (CRTA 2022a), which in turn was out of step with the European-wide understanding of the war.

Very interesting analyses documenting the way Serbian media report on events in Ukraine were provided by CRTA, which monitored the main Serbian media during the first months of the Russian aggression, namely from February 2022 to the end of May 2022, in two of its analyses (CRTA 2022a, 2022b). Generally speaking, one can observe a reticence in the assessment of the conflict in Ukraine in the first months of the conflict, but according to the authors, this can be explained by the circumstances that accompanied the incursion of Russian troops on Ukrainian territory. However, after the initial shock caused by this incursion, one can observe a rather biased reporting of the events on the Ukrainian battlefield, with one of the most traditional Serbian daily newspapers siding with Russia from the very first moments. On the day of the start of the Russian invasion, the Informer carried a catch-all headline on its front page titled "Ukraine attacks Russia!" as if it completely ignored reality. Then, on February 25, one of the traditional Serbian newspapers, *Večernje novosti*, carried a report on its front page that said, "Russia attack as a response to NATO's threat," which just goes to show how

Serbian newspapers have adopted the narratives appearing in the Russian media space. Another headline in the daily newspaper *Objektiv* predicted an easy victory for Moscow with the words: "Russians overran Ukraine in a Day" (CRTA 2022a). At this point, it is worth adding that as much as one-third of all disinformation in the Serbian media space comes from the newspaper *Večernje novosti* (CRTA 2022a).

What is evident in these analyses is that they quite clearly adopt the narratives that appear in the Russian media. An example is the false information that there are fascists in Ukraine against whom Russia is fighting. This narrative is commonly found in the Russian media (Drugă 2022) and the Serbian ones readily adopt it, as was evident in one of the headlines of a Serbian daily newspaper. Similarly, Serbian media emphasised that the Serbian government was under pressure from the EU for refusing to adopt sanctions against Russia, which is linked to interrupted Russian gas supplies to Europe (CRTA 2022b).

Generally speaking, a change in the topics of the Russian disinformation campaign can be observed in the Serbian media space. In addition to the traditional themes of denigrating the West and Euro-integration structures and defending Serbian interests in Kosovo, the Kremlin seems to have focused on getting Serbian society to adopt the Russian narrative regarding the Russian attack on Ukraine so that the legitimacy of this political move by the Russian Federation is not questioned. The fact that Serbian society has uncritically accepted the Russian interpretation of events is evidenced by the unwavering support for Russia in the country.

The question remains, what is the impact of Russian disinformation campaigns on public opinion in Serbian society in relation to the EU and NATO? Is the Kremlin succeeding in pursuing its foreign policy goals through disinformation? Frankly speaking, in the event of Serbia's possible accession to NATO, Moscow may not even try too hard to dissuade Belgrade from possible membership. According to analysts, the alienated attitude of Serbian society towards NATO is due to the fact that Serbia went through a bombing by this very organisation in the late 1990s (Radoman 2021). The Kremlin is trying to take full advantage of this fact in spreading its narratives, which are directed mainly against NATO and the US. Indeed, this fact not only increases tensions in Serbian society but also pits the peoples of the other Western Balkan states against each other (Metodieva 2019). The extent to which Serbian society's relationship with NATO is problematic is best illustrated by the fact from an opinion poll in which 68% of respondents expressed the view that NATO is the main culprit of the conflict in Ukraine. In addition, 82 respondents expressed themselves in the sense that they were against Serbia adopting sanctions against Russia (Hoxhaj 2022). However, given the historical reminiscences, this is not so surprising, as distrust toward NATO is deeply rooted in Serbian society. This is evident from a survey conducted in October 2022

on a sample of more than 1,000 Serbian respondents. In this survey, 62% of people expressed themselves in terms of not supporting Serbia cooperating with NATO in any way. However, two years earlier, in 2020, only 35% of respondents did so (Vuksanovic et al. 2022a). It is worth asking what could be behind such a steep decline in support for this option. Given the fact that there is an ongoing war in Ukraine, which in the eyes of Serbs was provoked by the North Atlantic Alliance, the answer is directly offered.

Even with EU support, the situation has not improved much, despite economic support from the EU over that from Moscow. The latest Demostat opinion poll clearly shows that the majority of the Serbian society prefers cooperation with Russia (namely 22% of respondents), while only 20% of respondents prefer cooperation with the EU. Similarly, in light of the events in Ukraine, 43% would prefer to maintain good relations with Russia, even if it means being forced to leave the EU (Demostat 2023). According to the same survey (May 2023), only a third of respondents would support the country joining the EU in a possible referendum (Demostat 2023). From this point of view, it can be concluded that the Kremlin is succeeding in stirring up anti-Western sentiment in Serbian society, and thus one of its geopolitical goals, that is, to keep Serbia out of the EU and NATO, has been successfully fulfilled so far.

Conclusion

This chapter has attempted to capture the most salient features of Russian narratives in the Serbian media space and to situate the Russian disinformation campaign in Serbia within the broader framework of SDIOs. As it becomes evident, Russia's disinformation seeks to interpret reality differently and, through its narratives, attempts to convince Serbs that it is acting as a victim in the environment of international relations, forced to defend itself through military means. These efforts by the Kremlin, according to the authors of this chapter, have a direct impact on Serbian public opinion.

More than ever, social media are being used, often deepening the divisions between different segments of the population. Set in the context of SDIOs, it is clear that two factors in particular are involved in the value destabilisation of Serbia. The first factor is the incompetent Serbian government, whose actions facilitate the spread of Russian narratives and create conditions for journalists that are far from the democratic ideal. The second factor is the positive attitude of Serbian society toward Russia, which further strengthens Russian narratives in this country and thus undermines the democratic and pro-Western direction of this Western Balkan country. This in itself allows Russia to spread pro-Russian narratives, to undermine the democratisation process in Serbia and, last but not least, to sow discord across Serbian society, which is exactly what Russia is seeking to do.

Notes

1 The pioneer of this concept is Frank Hofmann who claims that hybrid warfare "incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics, and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder" (Hoffman 2007, 8).
2 The monopoly in the Serbian media space has been created even though over 2,500 media platforms operate throughout Serbia (Reporters Without Borders 2024).

References

Amazeen, M. A., & Bucy, E. 2019. Conferring resistance to digital disinformation: The inoculating influence of procedural news knowledge. *Journal of Broadcasting & Electronic Media* 63(3): 415–432.

Bajic, D., & Zweers, W. 2020. *Declining MEDIA Freedom and Biased Reporting on Foreign Actors in Serbia*. The Hague: Clingendael Report, European Policy Center.

Balkan Barometer. 2020. *Analytical Report*. Regional Cooperation Council. Accessed January 29, 2024. https://www.rcc.int/pubs/95/balkan-barometer-2020-public-opinion-survey

Balmas, Meital. 2014. When fake news becomes real: Combined exposure to multiple news sources and political attitudes of inefficacy, alienation, and cynicism. *Communication Research* 41(3): 430–454.

Bjola, Corneliu, & Manor, I. 2021. Digital propaganda as symbolic convergence: The case of Russian ads during the 2016 US Presidential Election. In *Research Handbook on Political Propaganda*. Edward Elgar Publishing, 80–97.

Cendic, Kristina, & Gosztonyi, G. 2020. Freedom of expression in times of Covid-19: Chilling effect in Hungary and Serbia. *Journal of Liberty and International Affairs* 6: 14–29.

CRTA. 2022a. *Serbia Media Reporting on Ukraine Crisis*. CRTA. Accessed January 27, 2024. https://crta.rs/wp-content/uploads/2022/02/CRTA-Ukraine-in-Serbian-media-Media-Monitoring-Jan20-Feb20–2022.pdf

CRTA. 2022b. *Tracking the Propaganda and Disinformation about Foreign Influence in Serbia – Case Study*. CRTA. https://crta.rs/wp-content/uploads/2022/07/TRACKING-THE-PROPAGANDA-AND-DISINFORMATION-ON-FOREIGN-INFLUENCE-IN-SERBIA_CASE-STUDY.pdf

Demostat. 2023. *Public Opinion of the Citizens of Serbia – Omnibus May 2023*. Demostat: Research and Publishing Center. Accessed January 26, 2024. https://demostat.rs/upload/Demostat_Presentation_Jun%202023_English.pdf

Djuric, Rade. 2022. *Serbia Indicators on the Level of Media Freedom and Journalists' Safety 2021*. Safejournalist. Accessed January 29, 2024. https://safejournalists.net/wp-content/uploads/2023/07/SRB-ENG–2022.pdf

Doncheva, Tihomira. 2020. *Russia's Narratives toward the Western Balkans: Analysis of Sputnik Serbia*. NATO Strategic Communications Centre of Excellence, 77 pp.

Drugă, Dana Ionela. 2022. War in Ukraine: Russian propaganda themes. *Strategic Impact* 84+ 85: 80–93.

Duffy, M., & Green, S. 2020. *Organised Chaos: Russian Influence and the State of Disinformation in the Western Balkans*. Medford: The Edward R. Murrow Center for a Digital World.

Durach, F., Bârgăoanu, A., & Nastasiu, C. 2020. Tackling disinformation: EU regulation of the digital space. *Romanian Journal of European Affairs* 20(1): 5–20.

European Commission. 2022. Serbia 2022 report. *European Commission*. October12.https://neighbourhood-enlargement.ec.europa.eu/document/download/

d87e4167–65fd-42b0–8ede-7fa05c3d9355_en?filename=Serbia%20Report%20
2022.pdf
European Commission. 2023. Serbia 2023 report. *European Commission*. November 8. https://neighbourhood-enlargement.ec.europa.eu/document/download/9198cd
1a-c8c9-4973-90ac-b6ba6bd72b53_en?filename=SWD_2023_695_Serbia.pdf
Foreign Policy Concept of the Russian Federation. 2008. The Foreign Policy concept of the Russian Federation approved by Dmitry A. Medvedev, President of the Russian Federation. *President of Russia*. July 12. https://russiaeu.ru/userfiles/file/
foreign_policy_concept_english.pdf
Foreign Policy Concept of the Russian Federation. 2016. The Foreign Policy concept of the Russian Federation approved by Vladimir Putin, President of the Russian Federation. *President of Russia*. November 30. https://interkomitet.
com/foreign-policy/basic-documents/foreign-policy-concept-of-the-russian-federation-approved-by-president-of-the-russian-federation-vladimir-putin-on-november-30–2016/
Foreign Policy Concept of the Russian Federation. 2023. The Foreign Policy concept of the Russian Federation approved by Vladimir Putin, President of the Russian Federation. *President of Russia*. March 31. https://mid.ru/en/foreign_policy/
fundamental_documents/1860586/
Giles, Keir. 2016. Russia's 'new' tools for confronting the West-continuity and innovation in Moscow's exercise of power. [Research Paper]. *Chatham House*. March. https://
www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power
Godfroid, A. 2023. Aleksandra Godfroid: Serbian media and the war in Ukraine. *OBCT*. June 27. https://www.balcanicaucaso.org/eng/Areas/Serbia/
Aleksandra-Godfroid-Serbian-media-and-the-war-in-Ukraine–225960.
HLEG. 2018. A multi-dimensional approach to disinformation: Report of the Independent High Level Group (HLEG) on fake news and online disinformation. *European Commission. Publications Office of the European Union*. March. https://op.europa.
eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/
language-en
Hoboken, V. J., Appelman, N., Ó Fathaigh, Leersen, P., McGonagle, M., van Eijk, N., & Helberger, N. 2019. The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising. *Institute of Information Law, Faculty of Amsterdam*. Final Report.
Hoffman, F. G. 2007. *Conflict in the 21st century: The rise of hybrid wars* (p. 51). Arlington, VA: Potomac Institute for Policy Studies.
Hoxhaj, Andi. 2022. Ukraine war: Serbia is shifting closer to Russia – here's why. *Conversation*. November 7. https://theconversation.com/ukraine-war-serbia-is-shifting-closer-to-russia-heres-why-192472
Kapantai, E., Berberidis, C. A., & Peristeras, V. 2021. A systematic literature review on disinformation: Toward a unified taxonomic framework. *New Media & Society* 23(5): 1301–1326.
Karlsen, G. H. 2019. Divide and rule: Ten lessons about Russian political influence activities in Europe. *Palgrave Communications* 5(1): 1–14. https://doi.org/10.1057/
s41599-019-0227-8.
Kisic, I. 2022. The pro-Russian Media Campaign in Serbia. *Atlantic Initiative*. March 21. https://atlanticinitiative.org/the-pro-russian-media-campaign-in-serbia/#_ftn3
Kleut, J. 2022. *Mapping Disinformation in the Serbian Media in 2020. Research Report*. CRTA. https://crta.rs/en/mapping-disinformation-in-serbian-media-2020/
Knezevic, J. 2022. Russia's information warfare against the West in Serbia and the Western Balkans. *Mondointernazionale*. October 20. https://mondointer-

nazionale.org/en/focus-allegati/russias-information-warfare-against-the-west-in-serbia-and-the-western-balkans.
Littau, J., & Stewart, D. R. 2015. Truthiness and second-level agenda setting: Satire news and its influence on perceptions of television news credibility. *Electronic News* 9(2): 122–136.
Media Ownership Monitor. 2023. *Pressure on Truthful Reporting: Decline in Media Freedom in Serbia*. Accessed February 4, 2024. https://serbia.mom-gmr.org/en/findings/indicators/.
Media Ownership Monitor. 2024. *New Media Laws Have Legalized State Ownership of Media*. Accessed February 10, 2024. https://serbia.mom-gmr.org/en/findings/transparency/.
Merriam-Webster Dictionary. 2024. *Disinformation Noun*. Merriam-Webster. Accessed February 10, 2024. https://www.merriam-webster.com/dictionary/disinformation
Metodieva, A. 2019. *Russian Narrative Proxies in the Western Balkans*. German Marshall Fund of the United States. https://www.gmfus.org/sites/default/files/Russian%2520Narrative%2520Proxies%2520in%2520Balkans.pdf
Milutinovic, I., Djuric, R., Pavlovic, J., & Babic, M. 2023. Monitoring online media in the digital era. Application of the media pluralism monitor in the European Union, Albania, Montenegro Republic of North Macedonia, Serbia & Turkey in the year 2022. Country report: Serbia. *Centre for Media Pluralism and Media Freedom*. https://cadmus.eui.eu/bitstream/handle/1814/75736/serbia_results_mpm_2023_cmpf.pdf?sequence=1&isAllowed=y
Myhre, M. H., Aasland, A., & Holm-Hansen, J. 2024. Crimea will forever be Russian': Dissenting Norwegian media discourses on Russia's annexation of Crimea. *European Politics and Society* 25(1): 185–208.
Radoman, J. 2021. *Military Neutrality of Small States in the Twenty-First Century: The Security Strategies of Serbia and Sweden*. Springer Nature.
RATEL. 2023. *An Overview of the Electronic Communications Market in the Republic of Serbia. The Third Quarter of 2023*. Regulatory Agency for Electronic Communications and Postal Services. Accessed February 1, 2024. https://www.ratel.rs/uploads/documents/empire_plugin/Q4%202022.pdf
Reporters Without Borders. 2023a. *Europe – Central Asia. Press Freedom in Europe Overshadowed by the War in Ukraine*. Accessed February 2, 2024. https://rsf.org/en/classement/2023/europe-central-asia
Reporters Without Borders. 2023b. *Serbia Index 2023*. Accessed February 2, 2024. https://rsf.org/en/country/serbia
Reporters Without Borders. 2024. *Serbia: Media Landscape*. Media Landscapes, European Journalism Centre. https://medialandscapes.org/country/pdf/serbia
Secrieru, S. 2019. Russia in the Western Balkans. *European Union Institute of Security Studies* 2: 3–4.
Speranza, L. 2020. *A Strategic Concept for Countering Russian and Chinese Hybrid Threats*. Washington, DC: Atlantic Council.
Statista. 2024. *Share of People Who Would Vote to Stay in NATO If There Was a Referendum in Central and Eastern Europe (CEE) in 2023, by Country*. Statista. Accessed February 8, 2024. https://www.statista.com/statistics/1282208/opinion-on-staying-in-nato-in-cee-by-country/.
Tambini, D. 2020. *Media Freedom, Regulation and Trust: A Systematic Approach to Information Disorder*. Council of Europe Conference of Ministers Responsible for Media and Information Society.
TASS. 2022. 85% of Serbians will always support Russia whatever may happen – President Vucic. *TASS*. February 21. https://tass.com/world/1407763.

TASS. 2024. 'A friend in need is a friend indeed' – Vucic on relations of Russian, Serbian people." *TASS*. February 20. https://tass.com/world/1748789.

Törnberg, P. 2018. Echo chambers and viral misinformation: Modeling fake news as complex contagion. *PLoS ONE* 13(9): 1–21.

Vosoughi, S., Roy, D., & Sinan, A. 2018. The spread of true and false news online. *Science* 359(6380): 1146–1151.

Vuksanovic, V., Cvijic, S., & Samorukov, M. 2022a. Beyond Sputnik and RT: How does Russian soft power in Serbia really work? *Belgrade Centre for Security Policy*. https://bezbednost.org/wp-content/uploads/2022/12/How-does-Russian-soft-power-in-Serbia-really-work.pdf

Vuksanovic, V., Steric, V., & Bjelos, M. 2022b. Public perception of Serbian Foreign Policy in the midst of the war in Ukraine. *Belgrade Center for Security Policy*. December. https://bezbednost.org/wp-content/uploads/2022/12/Public-Perception-of-Serbian-Foreign-Policy-in-the-Midst-of-the-War-in-Ukraine.pdf

Walton, Calder. 2019. Spies, election meddling, and disinformation: Past and present. *Brown Journal of World Affairs* 26: 107.

Wardle, C., & Derakhshan, H. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking* (Vol. 27, pp. 1–107). Strasbourg: Council of Europe.

Wenzel, M., Stasiuk-Krajewska, K., Macková, V., & Turková, K. 2024. The penetration of Russian disinformation related to the war in Ukraine: Evidence from Poland, the Czech Republic and Slovakia. *International Political Science Review* 45(2): 192–208.

World Economic Forum. 2018. *Global Risks Report*. 13th ed. Geneva, pp. 48–50. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Zivotic, I., & Obradovic, D. 2022. Spread of the Russian propaganda on Western Balkans-case study in Serbia. *Security Horizons* 173.

12

THE TRANSNATIONALISATION OF STRATEGIC DIGITAL INFORMATION OPERATIONS

Turkey and India

Ihsan Yilmaz, Priya Chacko, Susan de Groot Heupner, and Anand Sreekumar

Introduction

SDIOs have increasingly drawn scholarly attention for their role in shaping digital authoritarianism through content-based, language-specific, cross-platform, and multimedia strategies. While much of this literature concentrates on domestic digital repression, less attention has been paid to the *transnationalisation* of SDIOs – how authoritarian regimes project digital influence across borders to mobilise diasporas, control narratives, and silence dissent. This chapter contributes to this emerging field by examining how Turkey and India, two assertive authoritarian regimes, deploy SDIOs transnationally as part of their broader authoritarian populist agendas.

In both contexts, diasporas are instrumentalised not only for diplomatic and economic purposes but also as extensions of the state's ideological and political apparatus. In Turkey, the state religious authority, Diyanet, has increasingly been used to govern Turkish citizens abroad and monitor dissenting voices (Maritato 2020). In India, the BJP has cultivated long-standing religious and diasporic networks to promote a vision of a "Bhakt nation," mobilising the Hindu diaspora in alignment with Modi's nationalistic and religiously inflected political project (Mathew 2021). In both cases, diasporas are repositioned as sovereign extensions of the homeland, committed to a sacralised nation (Mathew 2021).

Recent literature on transnational repression has highlighted a broad repertoire of coercive tools used to silence opposition abroad, including intimidation, censorship, rendition, and, in extreme cases, assassination (Schenkkan 2020a, 2020b). While such practices predate the digital age, digital technologies now provide authoritarian regimes with unprecedented capacity to

DOI: 10.4324/9781003628088-16
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

surveil, trace, and punish dissent across borders. The deployment of spyware such as Pegasus has enabled authoritarian actors to track diaspora members and critics in contexts where traditional state coercion would otherwise be difficult or illegitimate (Michaelsen 2020). Tactics including phishing, malware, doxing, online harassment, and disinformation now facilitate not only repression but also psychological control, generating a climate of fear and self-censorship among critics and exiles (Michaelsen 2020).

Adamson and Tsourapas (2020) define such practices under the rubric of transnational authoritarianism – the extension of domestic repression beyond borders through direct and indirect coercive means. Of particular relevance here is their notion of "coercion-by-proxy," in which pressure is exerted on citizens at home to indirectly target critics abroad, creating a low-cost mechanism of control that avoids violating host state sovereignty (Adamson and Tsourapas 2020).

Central to these operations is the control and manipulation of digital information. Digital authoritarian regimes increasingly rely on propaganda, conspiracies, malinformation, disinformation, and fake news to construct what has been termed an "information disorder" (Jones 2022). What distinguishes SDIOs from conventional propaganda is the hybrid use of digital technologies – especially artificial intelligence and algorithmic filtering – to engineer public sentiment and consent. The intent behind SDIOs is strategic and malign: to suppress dissent, amplify regime narratives, and construct a reality conducive to authoritarian control. Their accessibility and deniability make them especially attractive to both state and state-sponsored non-state actors (Jones 2022).

Social media plays a pivotal role in facilitating SDIOs. Research has shown that both authoritarian and democratic states use social media manipulation to target domestic and foreign audiences alike (Bulut and Yoruk 2017). Authoritarian actors deploy content-based strategies (e.g., hashtag flooding, meme wars), language-based tactics (e.g., native-language trolling), and multimedia coordination to target specific communities and exploit platform dynamics (Merhi et al. 2023). Nearly all authoritarian regimes in their global study engaged in domestic-targeted social media campaigns, while most democracies targeted foreign audiences (Merhi et al. 2023).

This chapter employs the SDIO framework to compare how the Indian and Turkish governments operationalise transnational digital repression and propaganda. It maps out the tools, actors, platforms, and discursive strategies used to construct and disseminate authoritarian narratives across borders. In both countries, SDIOs are integral to authoritarian populist governance, serving to suppress opposition, manipulate public opinion, and cultivate transnational legitimacy. These operations are executed by a wide network of actors, including IT cells, trolls, diaspora groups, party loyalists, media allies, and online communities of "genuine believers" (Yilmaz et al. 2023, 2).

Our methodological approach is based on desk research conducted by native Hindi and Turkish researchers, drawing on English and native-language media sources, institutional reports, and academic studies. The identified tactics were reviewed for saturation and validity by academic experts in both country contexts.

Our findings underscore that SDIOs are enabled by anti-democratic laws, surveillance regulations, and the complicity of domestic and transnational actors, including private-sector intermediaries. In both India and Turkey, SDIO targets extend far beyond borders, encompassing not only diaspora communities but also foreign journalists, academics, and politicians deemed hostile to the ruling party. By surveilling, intimidating, and delegitimising dissent across borders, these regimes extend the reach of authoritarian governance into digital diasporic spheres – undermining global norms of free expression and democratic pluralism in the process.

SDIOs in Turkey

This section offers a continuation of the analysis presented in Chapter 7, which detailed the Erdogan regime's emotional and symbolic political mobilisation strategies through digital platforms. Here, we summarise Turkey's evolution into a model case of mature digital authoritarianism, where SDIOs serve both domestic repression and transnational projection.

Between the 2013 Gezi Park protests and the 2016 coup attempt, Turkey experienced an intense erosion of internet freedom and rapid consolidation of authoritarianism under the AKP. Once a promising EU candidate and widely considered a democratic exemplar in the Muslim world, Turkey has increasingly used digital infrastructure to monitor, manipulate, and muzzle dissent. The collapse of its EU accession prospects, the securitisation of political life, and rising populist nationalism provided fertile ground for this authoritarian turn. By 2021, Turkey was ranked "not free" in democratic rights and internet freedom (Freedom House 2021).

Following the coup attempt, the digital sphere was securitised in tandem with broader crackdowns on civil society, journalists, academics, and political opposition. With over 80% of citizens online daily, spending an average of 7.5 hours connected (Bianet 2020), platforms like Facebook, Twitter (now X), YouTube, and Instagram became battlegrounds for influence. The AKP swiftly expanded its SDIO apparatus to counter opposition messaging and shape public perception (Bellut 2021).

Chapter 7 outlined how the regime relies heavily on emotionally charged messaging, using religious nationalism, historical victimhood, and identity politics to delegitimise rivals and galvanise its base (Yilmaz and Shipoli 2022; Yilmaz et al. 2023). These rhetorical devices are amplified by an extensive troll ecosystem: coordinated digital actors that praise Erdoğan, attack critics,

and manipulate online discourse (Saka 2018). Digital lynching – a term used to describe state-aligned harassment – targets journalists, artists, academics, and opposition figures with orchestrated abuse (Bulut and Yoruk 2017).

Trolls and bots – some operated by party cadres, others by graduates of pro-regime religious schools – deploy hashtags like #Milliİrade (national will), #CHPPKKnınİzinde (CHP follows the PKK), and #YerliVeMilli (local and national) to promote binary narratives and emotional manipulation. These operations tap into religious, nationalist, and conspiratorial tropes to foster a siege mentality and demonise dissenters as internal traitors, Gülenists, or foreign agents.

The regime's SDIO activities also have a transnational scope. As detailed in Chapter 7, pro-Erdogan accounts mobilise across languages – English, Indonesian, Persian, Somali, Russian – spreading hashtags such as #WeLoveErdogan and #ErdoganIsTheLeaderOfTheWorld. These efforts are not only about domestic image management but intended to generate global legitimacy and intimidate diaspora critics (Yilmaz et al. 2023).

The SDIO apparatus involves both automated and human agents. In 2020, Twitter removed over 7,300 Turkish propaganda accounts linked to coordinated disinformation, responsible for 37 million tweets supporting Erdoğan and vilifying opposition parties (Twitter Safety 2020).

Fake personas and pseudonymous accounts have also been used by senior AKP politicians, sometimes with comical missteps. Several officials, including AKP MP Ahmet Hamdi Çamlı and Minister Mehmet Özhaseki, mistakenly posted self-praising messages from their verified accounts – forgetting to switch to fake ones. Accounts like @Baskentci and @WakeUpAttack have circulated hit lists of journalists and false intelligence, signaling unofficial coordination with state actors.

As noted in Chapter 7, digital repression also operates through conspiratorial narratives. These include demonising critics of the government as members of fabricated threats – for example, the Gülen movement as CIA-linked conspirators, Gezi Park protesters as agents of foreign lobbies, and opposition candidates as PKK sympathisers. Trolls capitalise on public anxiety and polarised identity politics to promote hashtags like #EkrandakiYalancı (liar on TV) or #CHPyeKırmızıKart (red card to CHP), pushing disinformation as legitimate discourse (Elmas et al. 2019).

Critics of the regime – journalists, lawyers, academics – face disproportionate legal scrutiny. Meanwhile, regime-aligned digital actors operate with impunity. As noted by Human Rights Watch (HRW 2020), harassment campaigns frequently involve the leaking of personal information, doctored videos, or fabricated accusations. These tactics are intended to intimidate, silence, and isolate opposition voices.

In sum, Turkey's model of SDIOs reflects an integrated and strategic approach to digital authoritarianism. It combines state resources, party organisations, media infrastructure, bots, and trolls into a coherent system

designed to extend political control, influence information ecosystems, and project ideological legitimacy – both at home and abroad.

Turkey's Transnational SDIOs

The failed July 2016 coup marked a turning point in how President Recep Tayyip Erdoğan's government projects power beyond Turkey's borders. In its aftermath, Ankara launched an unprecedented campaign of transnational repression and digital information control targeting perceived enemies abroad. Initially focused on purging the Gülen movement (blamed for the coup), this effort soon widened to include Kurdish activists, critical journalists, and other dissidents across at least 31 countries. It combines online censorship, state-sponsored disinformation, intimidation of critics overseas, and co-optation of diaspora networks. The goals are to silence dissent within the diaspora and international civil society, shape favorable narratives, and promote Erdoğan's image while discrediting opponents.

Since 2016, Turkish authorities have significantly expanded their extraterritorial reach, employing tactics ranging from pressuring social media platforms to remove content, to disseminating propaganda through state media and "troll armies," to abducting or harassing exiled opponents.

Censorship of Dissent on Social Media

Ankara has used aggressive social media censorship as a key tool to silence overseas dissent. Turkish authorities frequently request the removal or blocking of content critical of the government, even if posted from abroad. According to Twitter's transparency data, Turkey ranked third globally for content removal requests in the first half of 2021 – behind only Japan and Russia (China excluded due to Twitter's ban). During this period, governments issued over 43,000 legal demands affecting nearly 197,000 accounts, with Turkey accounting for a significant share. Twitter's vice president for public policy called the rise in takedown requests "a deeply worrying trend" and a global "threat to privacy and freedom of expression." By targeting critical posts and accounts, Ankara seeks to sanitise platforms like Twitter, Facebook, and YouTube for Turkish and diaspora audiences.

Turkish courts routinely issue sweeping censorship orders affecting diaspora voices and foreign press. In early 2023, a court ordered the blocking of 69 journalists' Twitter (X) accounts on vague charges of terrorist organization propaganda. Among them was exiled journalist Amberin Zaman, whose account was geoblocked in Turkey at the government's request. Zaman noted that her tweets were innocuous, yet Twitter, under Elon Musk's ownership, complied. Many other diaspora journalists, Kurdish activists, and civil society figures have faced similar restrictions. In 2022 alone, Turkish courts issued at least 393 rulings to restrict access to about 4,427 Twitter

items – many critical of government officials (Freedom House 2023). These included posts alleging corruption or torture and statements from opposition figures. Through legal and technical means, Ankara scrubs unfavorable content from the Turkish internet, creating a form of digital exile in which critics abroad are rendered invisible to domestic audiences.

Beyond court orders, Ankara also pressures social media companies behind the scenes. Firms like Twitter face a stark choice: risk being banned in Turkey or comply. Most choose compliance. Ahead of the May 2023 elections, Twitter censored specific accounts and tweets globally at Ankara's request, drawing criticism for enabling censorship on an international platform. The pattern is clear: Turkey leverages its market size and legal tools to export censorship, making dissenting posts from London or Berlin disappear from Turkish cyberspace if they challenge Erdoğan's narrative.

State-Linked Troll Armies and Disinformation Campaigns

While silencing dissent, Ankara simultaneously promotes its own narratives through coordinated online campaigns. Social media "troll" networks amplify regime messaging, a strategy developed after the 2013 Gezi Park protests revealed the importance of dominating online discourse. In response, Erdoğan's AKP cultivated a troll army – reportedly organised by presidential advisers – to flood platforms with pro-government content and harass critics. Leaked 2016 emails detailed plans to recruit "professional graphic designers, coders and former army officials trained in psychological warfare" to influence public opinion. These fake or pseudonymous accounts, dubbed "AK Trolls," have been active since 2013–2014, supporting Erdoğan's narratives and attacking opponents. Studies show their increasing sophistication, with coordinated hashtag campaigns and astroturfing efforts. During crises – such as military operations in Syria or official scandals – thousands of inauthentic or loyalist accounts saturate Twitter and Facebook with government talking points to drown out alternative views. This was evident after the December 2016 assassination of Russia's ambassador in Turkey, when pro-government troll farms pushed false claims blaming Gülenists to deflect attention from jihadist links (Bozkurt 2020).

Government officials openly back these influence efforts. In 2022, Turkey's Communications Directorate, led by Fahrettin Altun, established a "Center for Combating Disinformation" (DMM) to counter so-called "fake news" about Turkish policies. The DMM publishes multilingual bulletins to refute allegations of human rights abuses, corruption, or military misconduct, swiftly promoting the state's version of events. These bulletins – disseminated in English, German, French, Russian, and Arabic – reframe sensitive issues like terrorism probes or civilian casualties. By labeling critical reports as "misinformation," the state engages in international perception management.

Turkey's digital influence operations also extend into cyber campaigns. Pro-Erdoğan hacker groups have targeted foreign entities to spread Ankara's message. In March 2017, amid tensions with Europe, a Turkish hacktivist group hijacked numerous high-profile Twitter accounts – including those of politicians, CEOs, media outlets, and NGOs – replacing content with pro-Erdoğan slogans and Nazi-era insults targeting Germany and the Netherlands. Messages featured Nazi symbols, Turkish slogans, and hashtags like #Nazialmanya ("Nazi Germany") and #Nazihollanda ("Nazi Holland"), referencing Turkey's 2017 constitutional referendum with "See you on April 16". Victims included the European Parliament, UK Department of Health, Die Welt, BBC North America, Reuters Japan, Amnesty International, and UNICEF. Separately, Turkish "hacktivists" have breached accounts of Western journalists to intimidate and spread propaganda. In 2018, the hacker group Ayyıldız Tim took over Twitter accounts of US media figures to post pro-Erdoğan messages, using tactics from defacements to denial-of-service attacks – blurring the line between cybercrime and state propaganda.

Platforms have attempted to push back. In June 2020, Twitter removed 7,340 accounts linked to a Turkish state-affiliated network that had posted over 37 million tweets promoting Erdoğan's AKP and targeting opposition (Harper 2020). Twitter attributed the network to the AKP's youth wing, confirming suspicions of organised manipulation (York 2020).

Harassment and Intimidation of Critics Overseas

Freedom House lists Turkey among the top perpetrators of transnational repression against exiled journalists, citing "digital harassment, smear campaigns, doxing, and other attempts to prevent truthful reporting" (Freedom House 2022). Harassment ranges from coordinated Twitter attacks – thousands of pro-government accounts targeting a critic with slurs and threats – to surveillance and threats against exiles and their families. Many Turkish journalists abroad assume their social media is monitored and that criticism could prompt retaliation.

Even diaspora citizens in third countries have been targeted (van der Noordaa 2020; Connolly 2016; Al Jazeera 2016). NGOs and human rights groups critical of Turkey have also been targeted. Officials routinely dismiss reports from Amnesty International or Human Rights Watch as "lies" or "terrorist propaganda," while pro-government media publish defamatory stories about these organisations.

Interference in Foreign Politics and Diaspora Surveillance

Turkey has directly intervened in diaspora politics and elections, treating the Turkish diaspora – over six million in Europe alone – as an electoral base.

Using social media, WhatsApp groups, and state-backed diaspora organisations, the Turkish government mobilised over 1.4 million expat voters in Europe, likely tipping the narrow referendum result in Erdoğan's favor (Taş 2018). Ahead of Turkey's 2023 elections, similar networks in Europe and North America mobilised expat votes and circulated negative propaganda against opposition candidates, branding them as weak or sympathetic to terrorists.

Ankara's digital interference has at times intersected with third-party disinformation. In early 2023, leaked documents revealed a Russian intelligence operation staging a fake anti-Turkey protest in Paris to provoke Erdoğan before the elections. Posing as a "Ukrainian community," actors desecrated a Quran during a staged protest, filmed the scene, and distributed it online. A week later, a Turkish pro-government outlet published an inflammatory article based on the footage – authored by a writer linked to Russian state media. The video spread rapidly on TikTok, Telegram, YouTube, and Facebook, especially in diaspora groups with large followings (Shakir et al. 2023). While the operation failed to influence the election, it highlighted how Turkey's politicised media ecosystem can be exploited by foreign actors when narratives align, in this case amplifying anti-Western sentiment among Erdoğan's base.

Turkey also interferes in foreign policy debates abroad by using diaspora voices and digital pressure. A key example came during Sweden and Finland's NATO accession process (2022–2023). Leveraging its veto power, Ankara demanded that both countries act against Kurdish and Gülenist exiles. In a June 2022 memorandum, Sweden and Finland agreed to "combat disinformation" and restrict funding to groups Turkey designates as terrorist (e.g., the PKK and Gülen network). Turkish officials maintained pressure via social media, accusing Sweden of "harboring terrorists" after every Kurdish protest. When exiled activists staged an anti-Erdoğan stunt in Stockholm, Ankara's media triggered a wave of online outrage and diplomatic protest, briefly endangering Sweden's NATO bid.

Co-opting Diaspora Organisations and Digital Nationalism

Central to Turkey's transnational strategy is the co-optation of diaspora organisations and the cultivation of digital nationalism among Turks abroad. Over the past decade, Ankara has invested heavily in "diaspora engagement," turning migrant communities into extensions of its political base. The Turkish state views Turks abroad as a source of domestic support and a tool to advance foreign policy goals (Öktem 2014; Legrello 2021). Ankara has also deliberately shaped diaspora identity politics to reinforce loyalty. Erdoğan and AKP officials often portray Turkish immigrants in the West as the "guardians" of Turkey's honor and the wider Muslim community (AP

2017). Erdoğan's global messaging often paints Turkey as the vanguard of Muslims and the oppressed, versus a morally bankrupt West (Yeşil 2024).

Digital platforms amplify this diaspora nationalism. Young diaspora Turks are often active on social media, and the Turkish government has sought to harness that energy online. During episodes like Turkey's cross-border incursions in Syria (e.g., the October 2019 operation against Kurdish forces), one could observe a surge of nationalist hashtags (#TurkeyWinning, #ErdoganStrong, etc.) propagated by users in Europe and North America alongside those in Turkey. Some of this was organic pride, but evidence shows a coordinated element – for instance, WhatsApp groups run by AKP supporters abroad disseminating templated messages and graphics for members to post on Facebook and Twitter (Karan 2020). The result is a chorus of digital cheerleading for Erdoğan's government emanating from accounts in Germany, the UK, the US, and elsewhere. Detractors in those same communities – for example, a Kurdish activist in London criticising the military action – may find themselves swarmed by commenters accusing them of treason or terrorism. This online peer pressure silences alternative diaspora voices while giving politicians back in Turkey the impression of widespread diaspora consensus (Hacaoglu 2020).

Promoting Erdoğan's Image and Smearing Opponents Abroad

Underlying Turkey's transnational SDIOs is a consistent dual narrative: projecting President Erdoğan and his ruling AKP in a positive, heroic light abroad, while actively discrediting and delegitimising any opponents or critics. This narrative is disseminated through every available channel – official speeches, international media, social networks, and diaspora events – to shape how global audiences perceive Turkey and its leadership.

There are recurring core narratives in Turkey's global communications: "Turkey as a benevolent force reshaping the global order; the West as morally bankrupt and declining; Muslims as victims of Western hegemony; and Turkish Muslim civilization as superior" (Yeşil 2024). These themes are reinforced in everything from TRT World documentaries to Erdoğan's UN speeches. The messaging serves to rally not only Turks but also Muslims abroad to admire Erdoğan as a pious, strong leader who stands up to a hypocritical West. This image crafting has been so assertive that by 2020 the AKP was hosting lavish rallies for Erdoğan in European cities (until host governments banned them), and slogans like "Erdoğan, voice of the oppressed" became common in pro-government discourse.

Conversely, the smearing of critics is relentless and closely intertwined with Turkey's counterterrorism narrative. The Turkish government labels virtually any significant opposition group or dissident movement as "terrorists" or traitors on the international stage (Jenkins 2018; Schenkkan 2020b).

Through op-eds, think-tank panels, and Twitter campaigns, pro-Erdoğan figures constantly try to link opponents (journalists, exiled politicians, NGO workers) to terrorism.

At the same time, Turkey's state media pumps out conspiracy theories to muddy the waters. It is not uncommon for outlets like *Daily Sabah* or TRT's various foreign-language services to run stories suggesting that critical diaspora groups or NGOs are funded by nefarious foreign powers (the CIA, "the interest lobby," or other bogeymen). This framing turns every Twitter argument with a Turkish exile, every critical article in *The New York Times*, into just another front in a grand information war against Turkey. And in that war, Erdoğan casts himself as commander-in-chief of the truth, while his detractors are portrayed as either misguided at best or malicious traitors at worst.

SDIOs in India

In India, the Bharatiya Janata Party (BJP) government has implemented a broad array of digital authoritarian practices, aimed at suppressing dissent and consolidating power. These include censorship attempts, internet shutdowns, and narratives.

The interventions censoring online content are typically justified on national security grounds and facilitated through close cooperation with social media platforms, driven by both commercial imperatives to maintain access to the Indian market and coercive regulatory mechanisms introduced by the state. Between 2015 and 2022, India blocked over 26,000 websites under Section 69A of the IT Act, a provision designed to protect public order and national sovereignty (The Wire 2023a). Many of these blocks aligned with ideological goals, targeting content advocating for Sikh independence, opposing Hindu nationalism, or supporting Kashmiri self-determination (Mihindukulasuriya 2021). In 2020, India submitted the highest number of global requests to Twitter for both content takedowns and user information (Freedom House 2023). By 2021, the Indian state escalated its efforts, demanding not only content removals but also the deletion of entire social media accounts, following widespread online mobilisation against the government's controversial agricultural laws and criticism of its handling of the COVID-19 pandemic. The new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 also required platforms to respond swiftly to takedown orders (Mehrotra and Menn 2023).

Beyond institutional mandates to platforms, the Ministry of Home Affairs launched a cybercrime volunteer program that encourages citizens to report "unlawful content" deemed harmful to India's integrity and social fabric (Chandran 2021). These digital repression efforts were further formalised in the IT Amendment Rules of 2023, which compel platforms to employ moderation tools, including AI, to block content that the government defines

as a threat to public order, decency, morality, or national integrity, or that constitutes "fake news" about the state. Crucially, the 2023 rules eliminate "safe harbor" protections that once shielded platforms from liability over third-party content, enabling the government to target critics without due judicial process (Freedom House 2023, 15; Karanicolas 2021).

India has also emerged as the global leader in the use of internet shutdowns. A regulatory framework introduced in 2017 has enabled BJP-led state governments to disrupt internet access at the district and municipal levels. These shutdowns are often justified in the name of quelling "communal tensions," yet such tensions are frequently instigated by BJP figures and affiliates using social media platforms to depict Muslims, Sikhs, Christians, and secular liberals as threats to India's unity and to Hindu society (Ruijgrok 2022; Shih 2023). Disinformation and misinformation are used to obscure incidents of violence against minorities and to incite further unrest.

The BJP and affiliated Hindu nationalist actors have operationalised a wide range of narratives online. Politicians and influencers – including figures like Amit Malviya – regularly disseminate content portraying Muslims as sexual predators, traitors, or agents of Pakistan, while framing Hindus as under existential threat. These narratives are often linked to broader conspiratorial discourses involving global elites like George Soros, opposition parties, or foreign governments (Banaji et al. 2019; Chaudhuri 2020; BJP 2023; Citizens and Lawyers Initiative 2020; Shih 2023; The Wire 2024b). Inauthentic social media activity – ranging from automated bots to fake accounts and disinformation networks – has also become central to electoral politics in India. The BJP has been particularly effective in leveraging such tactics. During the 2019 national election, covert digital assets linked to the BJP disseminated a flood of vitriolic posts attacking opposition leaders with fabricated quotes, accusations of corruption, and allegations of Hindu betrayal or Muslim favoritism (DFR Lab 2019; Patel and Chaudhuri 2019). These activities also extended to the 2020–2021 farmers' protests, seeking to glorify the Indian military and discredit protest leaders (Strick 2022).

India's Transnational SDIOs

These domestic SDIOs have also been deployed transnationally to quell dissent from the Indian diaspora and transnational organisations, surveil them as well as promote the aims of the BJP regime and Hindutva narratives abroad through influence operations.

Transnational Harassment of Dissidents

In 2020, a number of global sites, which were associated with resistance to Hindutva as well as the Kashmiri movement, were blocked (Mihindukulasuriya 2021). The recent ownership shifts in Twitter/X have only exacerbated

this trend with the censorship of two prominent international human rights advocacy organisations (Indian American Muslim Council and Hindus for Human Rights in India) in India in October (*Scroll* 2023). Similarly, a staggering 120 accounts (including foreign Sikh and minority accounts) were withheld on X in the wake of the government's requests amid its search for fugitive Sikh separatist leader Amritpal Singh Sandhu (Sharma 2023). Prior to the Indian elections in 2024, the websites or social media handles of Hindutva hate crime tracker websites like Hindutva Watch as well as India Hate Lab were blocked. The farmer's protests in India have also led to the censorship of a number of accounts and posts in X (Al Jazeera 2024a, 2024b).

Foreign media organisations have also been a target of censorship via social media. In 2022, the Indian government issued blocking orders to prevent the broadcasting of a BBC documentary questioning Narendra Modi's role in the 2002 Gujarat pogrom while opposition politicians who promoted the documentary had their posts taken down (Al Jazeera 2023). In 2024, two foreign documentaries and associated news stories, from Canadian and Australian broadcasters, were blocked on social media platforms related to the murder of Sikh separatist activist Hardeep Singh Nijjar (with alleged links to India) (*Scroll* 2024). The satirical YouTube Shorts video of Australian YouTube channel *The Juice Media*, titled "Honest Government Ad: India" illustrating the state of India's democracy, was also blocked in India in 2024 (The Wire 2024a; NT 2024).

Outspoken individuals have often been targeted by digital mobs, often traced back to right-wing Indian diaspora groups or pro-BJP trolls on platforms like Twitter and WhatsApp. One stark example was the online abuse campaign against Professor Mohan J. Dutta (and his colleagues), who published a research paper critical of Hindutva (Hindu nationalist) ideology in New Zealand in 2021 (*Newsroom* 2021). In an alarming twist, the official Twitter account of the Indian High Commission in Wellington abetted this harassment by sharing a misleading video that conflated Dutta's critique of Hindutva with an attack on Hinduism itself, effectively painting the academic as "Hinduphobic" (*Aotearoa Alliance of Progressive Indians* 2021). The term "Hinduphobia" is often wielded as "a political tool to silence opposition to Hindu nationalism rather than to address genuine discrimination against Hindus" (Arshad 2023). Across Western academia, scholars researching Indian politics or Hindu nationalism have encountered similar digital harassment. A Canadian Hindutva group "Dwarapalaka" even openly admitted to sending threatening emails to scholars (Swyers and Trinh 2022). The involvement of formal diaspora organisations indicates a degree of coordination and approval for these harassment campaigns, blurring the line between grassroots fanaticism and state-sponsored intimidation. Perhaps the most spectacular instance of transnational digital harassment was the ferocious backlash to the "Dismantling Global Hindutva" online conference

in September 2021, co-hosted by over 50 universities worldwide (mostly in the US). In response, a constellation of overseas Hindu nationalist groups launched a full-scale assault on the organisers and participants including death threats, misogynistic insults, and defacement of professional profiles. Central to the attackers' narrative was the accusation of Hinduphobia (Naik 2021) (Ellis-Petersen 2021). The fever pitch was such that US federal law enforcement became aware of the harassment, a rare acknowledgment in cases of diaspora-origin intimidation. The episode underscored how diaspora extremists, tacitly empowered by the Indian state's nationalist rhetoric, could reach across borders to enforce ideological conformity through intimidation.

Diaspora Surveillance and Influence Networks

Parallel to its harassment tactics, the Indian state has developed an infrastructure for surveilling diaspora communities (numbering over 30 million) and conducting influence operations abroad. A revealing case emerged in late 2023, when *The Washington Post* uncovered that an ostensibly independent American nonprofit called "The Disinfo Lab" was a front for an Indian intelligence operation. The Disinfo Lab (which billed itself as exposing propaganda) was secretly compiling detailed dossiers (including extensive personal information) on vocal foreign critics of the Modi regime or Hindu nationalism (Shih et al. 2023; Friedrich 2024). The Disinfo Lab also produced slick conspiracy reports attempting to link overseas critics to Pakistan's ISI or to George Soros's philanthropy, feeding into the BJP's narrative that any opposition to it is driven by shadowy foreign plots (Beauchamp 2024; The Wire 2024b). Notably, the disinformation output of this front organisation was eagerly amplified by the BJP's own social media ecosystem giving it an air of credibility (Shih et al. 2023). This synergy between espionage and propaganda illustrates how India's diaspora surveillance feeds directly into its IO: data gathered covertly are used to publicly discredit and intimidate prominent diaspora voices.

Indian diplomatic missions abroad have effectively become extensions of the regime's surveillance network. Officials in consulates have constantly surveilled local diaspora events (especially protests or conferences related to Kashmir, Sikh activism, or criticism of human rights in India), gurudwaras and community events at Indian embassies (Michaelsen 2020; Hussain and Grim 2023; Beauchamp 2024). Social media is also meticulously scoured for diaspora Indians voicing dissent. Those identified may get a quiet visit or call from an Indian official warning them to "correct" their behavior, or they might simply find out later that their visa to India has been revoked. To justify and facilitate this surveillance, Indian officials often push a narrative that any diaspora criticism equals support for extremism. For example, during the Leicester violence in the UK (2022) – clashes between some Hindu

and Muslim young men partly inflamed by social media rumors – the Indian High Commission in London issued a statement only decrying attacks on Hindu symbols, implicitly blaming Muslim communities and ignoring Hindu nationalist provocations. This one-sided account fed into the Hindutva narrative and set the stage for more surveillance of British Muslim activists under the guise of protecting diaspora Hindus (Al-Khalaf 2023; Abul and Pyke 2023). Similarly, in Canada, the Indian High Commission tweeted a doctored photo of a vandalised park sign (in what was falsely portrayed as a hate crime against Hindus), using it to suggest that Hindu sites in Canada were under attack by Sikh extremists. Canadian police later debunked the incident, but the misinformation bolstered India's claims that its diaspora (specifically Hindus) were in danger and thus increased surveillance was warranted (Niranjankumar 2022; The Wire 2023b). In both cases, official disinformation created a pretext for Indian authorities to demand greater oversight and action regarding diaspora affairs, forcing Western agencies to engage with Indian intelligence. The result is that activists of Indian origin in countries like Canada or the UK may find themselves on local law enforcement radars, due to Indian allegations, which is a troubling form of outsourced repression (Adamson and Tsourapas 2020).

In addition to surveillance, India runs influence networks through diaspora organisations to shape opinion and policy abroad. They include Overseas Friends of BJP (OF-BJP) chapters, as well as a plethora of ostensibly independent diaspora groups – cultural associations, business councils, and advocacy nonprofits – that align closely with the Indian government's interests. These networks have a significant impact in rallying diaspora support for the regime or in quieting dissenting voices, through physical as well as online means. In one telling episode, ahead of the 2024 Indian general election, a number of overseas pro-democracy organisations planned to run campaigns highlighting democratic erosion under Modi. Almost immediately, countermobilisation occurred: large-scale "#ModiForPM2024" rallies were organised in cities like Sydney and New York by diaspora groups, dwarfing the democracy campaign's reach and sending a message that Modi enjoyed vast non-resident Indian (NRI) support (*Livemint* 2024; *The Economic Times* 2024). One could see similar mobilisations in support of the *praan prathishta* (consecration) of the Ram *Mandir* (temple) at Ayodhya in January 2024. The consecration of the Ram Mandir, built at the site of the demolition of the Babri Masjid, was the culmination of a polarising and bloody decades-long campaign, intricately linked to the ascendance of Hindutva and the BJP in India (*VHP America (@VHPANews)/X* 2024; *India Today* 2024; *Rediff.Com* 2024). The end game is to project an image that the Indian diaspora is united behind the home government, thereby marginalising dissident diaspora voices and even influencing foreign politicians who court the diaspora vote bank.

Hindu nationalist organisations as well as diasporic ideologues (most prominently Rajiv Malhotra) have also spearheaded numerous online campaigns against interventions aimed at addressing caste discrimination against widespread evidence of the persistence of caste discrimination within India's global diaspora (Wilson 2017; Infinity Foundation Official n.d.). For instance, multiple Hindu Right groups in the US "proposed textbook edits designed to whitewash caste and patriarchy in ancient India and within Hinduism" through online campaign platforms like change.org (Punit 2016; Truschke n.d). Online petitions and social media/email campaigns are also often deployed to obstruct multiple caste legislation interventions in the US as well as to silence academics (including in Australia) (*Sign the Petition* 2023). Besides these obstructive and "constructive" campaigns, the YouTube channels of Hindu nationalist organisations like National Council of Hindu Temples (UK) have also sought to propagate the notion that caste is a colonial import and not intrinsic to Hinduism.[1]

Foreign Influence Operations

New Delhi has also pursued broader foreign influence operations to sway public opinion and policy in other countries and to reshape the international narrative about India and its adversaries. In many cases, the diaspora serves as a conduit or proxy for these operations.

One notable theatre of Indian influence has been the United Kingdom, where a large Indian-origin population and historical ties give India leverage. In late 2019, after the Indian government revoked Jammu & Kashmir's autonomy (Article 370) and cracked down in the region, the UK's Labour Party passed a resolution critical of India's actions. The BJP and its allies reacted swiftly: the Overseas Friends of BJP (OF-BJP) in the UK launched a campaign encouraging British Indians to switch their support to the Conservative Party, framing Labour as "anti-India" (Mathew 2022). This campaign coincided with a flood of disinformation on social media including doctored images depicting Labour leader Jeremy Corbyn as Hitler, and false rumors claiming London's Muslim mayor Sadiq Khan had banned Diwali celebrations. Sikh British MPs from Labour (like Tanmanjeet Singh Dhesi who had criticised human rights issues in India) were also targeted with fake news (Hundal 2019). By many accounts, the campaign had an impact: in the 2019 UK general election, Labour fared poorly in some districts with sizable Indian-origin populations, and analysts partially attributed this to the Kashmir issue backlash and associated influence operations (Hundal 2019). This case demonstrates how India can leverage diaspora networks and misinformation to affect political outcomes abroad when its core interests (or the ruling party's reputation) are at stake.

In the US, Indian foreign influence efforts have similarly piggybacked on diaspora organisations and political sympathisers. Under the Trump administration (2017–2020), the BJP found an unusual alignment with the American right, and diaspora conservative groups took full advantage. Organisations like "Hindus for Trump" held high-profile online and offline events. Reportedly, over 100,000 Indian-Americans participated in a 2020 virtual rally in support of Donald Trump which blended US Republican talking points with Modi-era Hindu nationalist themes (Financial Express 2020). Meanwhile, pro-BJP influencers on American social media propagated Islamophobic memes targeting Kamala Harris and casting the Democratic Party as "pro-Pakistan" or "anti-Hindu" (Pahwa 2020). These activities were not officially directed by the Indian state, but Indian diplomats notably did not discourage them; on the contrary, they often engaged with and praised diaspora supporters who lobbied US lawmakers on issues like Kashmir or sanctions relief. The cumulative influence has been substantial: the India lobby in Washington, once focused mainly on trade and tech relations, now frequently presses US officials to adopt the BJP's framing on human rights and minority issues (e.g., that outside critiques are exaggerated or motivated by bias). American lawmakers who speak up on Kashmir or Indian minority rights have faced orchestrated email/letter campaigns from diaspora groups defending India and sometimes smearing the lawmakers as sympathetic to terrorists. This soft power offensive has helped inoculate India to some degree from international censure. During Modi's state visit to the US in 2023, for instance, critical voices were drowned out by lavish praise from diaspora-led welcome events and glowing references to India as a strategic partner against China. US policymakers' public remarks conspicuously avoided mention of democratic backsliding in India, reflecting how effectively the narrative has been managed in the halls of power (Beauchamp 2024).

Australia has also seen Indian foreign influence efforts, typically channeled through diaspora mobilisation against media and academia. Indian officials and aligned diaspora groups have reacted vehemently to Australian media reports critical of Hindu nationalism. In 2023, after the Australian Broadcasting Corporation (ABC) ran investigative pieces on Hindutva activity in Australia, a consortium of Hindu organisations in Australia (with encouragement from Indian diplomats) organised protests and social media campaigns accusing the ABC of bias in the form of an "incessant stream of anti-India stories" (Australian Hindu Media n.d.a, n.d.b). The aggressiveness of the response was striking for an issue entirely within Australian domestic discourse; it signaled the reach of Indian influence networks in policing global narratives about India. Similarly, when an Australian university considered adding caste discrimination to its anti-discrimination policy (to protect lower-caste students in diaspora communities), Hindu groups in Australia mobilised online petitions opposing it, framing it as an attack on Indian culture (*Sign the Petition* 2023).

In Canada, the information war has been even more intense due to ongoing diplomatic rifts. Pro-India online networks have repeatedly targeted Prime Minister Justin Trudeau and his government with disinformation. During the 2023 G20 summit in Delhi, Trudeau's departure was delayed by aircraft technical issues; yet a wave of tweets and posts from Indian accounts spread the false story that drugs were found on his plane (Johal 2023). Astonishingly, this fake news was even echoed by a former Indian diplomat, blurring the line between fringe online rumors and official propaganda (The Wire 2022). Canadian officials noted that the incident was part of a pattern of online attacks on Canadian figures whenever Indo-Canadian relations became strained (Johal 2024). By flooding social media with derogatory narratives about Trudeau (depicting him as sympathetic to Sikh "terrorists" or personally compromised), these influence operations aimed to erode his credibility domestically and internationally. Further, a Canadian intelligence report tabled at the Public Inquiry into Foreign Interference revealed an extensive network of pro-BJP accounts and bots repeatedly targeting Canadian activists, politicians, and journalists. A notable example in this regard was the dissemination of a baseless rumor that a murder suspect linked to the murder of 37-year-old Paul Schmidt had attended a pro-Khalistan rally prior to the murder. This disinformation was spread by anonymous Twitter accounts and amplified by Indian media organisations in India. Even attempts to counter this misinformation were trolled heavily (Johal 2023).

There is also increasing evidence of politically motivated actors shaping the online environment in relation to geopolitical events and crises. For instance, after the revocation of Article 370, a network of inauthentic Twitter/X accounts amplified "misleading content showing local Kashmiris reacting favourable to the Indian government" seeking "to promote a positive view of the Indian government" and BJP policies, drowning out dissident voices through distractions (Zhang 2022). While there is insufficient open-source evidence to link this SDIO to a specific actor, research by the Stanford Internet Observatory suggests that this content is consistent with, and frequently mentioned/retweeted, the content of social media accounts of the Indian army's Kashmir unit, the Chinar Corps, which was suspended by Twitter/X and Meta during this time for inauthentic behavior (Grossman et al. 2022).

One of the most ambitious Indian foreign influence operations uncovered to date pertains to a Delhi-based network (later linked to the Srivastava Group) which ran a complex web of fake media outlets, think tanks, and NGOs across dozens of countries for 15 years (Machado et al. 2019). This network resurrected names of defunct organisations and fake personas "speaking" in favor of India. The content generated by these fake entities was then laundered through ANI – a major Indian news agency – which unwittingly or otherwise picked up the stories and fed them into Indian news streams. The aim was twofold: bolster India's image as a responsible global actor (e.g., highlighting supposed international praise for India or criticism

of its rivals) and discredit Pakistan (and to a lesser extent China) by accusing them of malfeasance on the international stage. Notably, the disinformation network also targeted institutions like the European Parliament: it organised delegations of far-right European lawmakers on trips to Kashmir under the pretense of fact-finding, giving them a curated pro-India experience (including meetings with Prime Minister Modi). These lawmakers would then return home and speak favorably of India's policies. The scale and duration of the Srivastava operation were unprecedented for India, spanning 116 countries and 550+ fake websites (Machado et al. 2019). While the Indian government denied any involvement, the fact that those involved had access to high-level Indian officials (as evidenced by the VIP Kashmir trips) suggests at least tacit approval.

India's foreign influence campaigns often intersect with its geopolitical interests and alliances. A contemporary example is how Indian information operators have aligned with pro-Israel narratives during conflicts in the Middle East. During the 2023 Israel–Hamas war, Hindu nationalist social media in India and abroad aggressively pushed anti-Palestinian and Islamophobic content, framing Israel's fight as analogous to India's fight against Islamist militancy (Dasgupta 2023). At the same time, BJP officials in India pounced on an October 2023 bomb blast in Kerala (India) to suggest, without evidence, that it was linked to Hamas – a way of smearing the local leftist government as naive on Islamist terror (Dasgupta 2023). Both threads of disinformation advanced complementary narratives: (a) global Islamist terror threatens democracies everywhere (implying criticism of India's policies equals support for terror) and (b) India and its allies (like Israel) share a righteous cause against this menace. Indian diplomats amplified these points in international forums, positioning India as a stalwart against terrorism, while domestic trolls attacked any pro-Palestinian sentiments as traitorous. This convergence of domestic propaganda with foreign policy messaging is a hallmark of India's strategic communications today. It allows the government to spin international events for domestic gain, and vice versa, to leverage domestic fervor for foreign policy advantage.

Conclusion

This chapter has demonstrated the expansive transnational reach and growing impact of SDIOs conducted by the Indian and Turkish governments. Far from being confined within national borders, these operations extend outward – targeting diasporic communities, transnational organisations, foreign media, and political actors abroad. As the cases of India and Turkey reveal, SDIOs serve multiple functions: they reinforce regime legitimacy at home, mobilise support within diasporic communities, and undermine opposition and minority groups both domestically and internationally.

Diasporas are strategically central to these operations. They represent vital sources of financial, electoral, and discursive capital. By influencing diaspora communities, governments aim to harness these communities' political, economic, and symbolic resources – while also using them to project soft power abroad. At the same time, diasporas become key sites of repression when they harbor dissenting voices. Our analysis shows that SDIOs are used to silence dissent, discredit alternative narratives, and intimidate critics through digital surveillance, targeted harassment, and disinformation campaigns.

These operations are embedded within an infrastructure of anti-democratic laws and regulatory mechanisms that provide legal cover for censorship, platform manipulation, and surveillance. Both states have enacted legislation that compels private companies – especially social media platforms – to comply with censorship and content moderation demands. The erosion of platform protections, combined with vague definitions of "public order" and "national integrity," allows the state to weaponise digital spaces without meaningful accountability.

Crucially, SDIOs are sustained by a broad network of actors. This includes pro-government diaspora organisations, party-affiliated IT cells, digital influencers, trolls, online vigilantes, and compliant journalists. Transnational governmental coordination and informal collaborations with private-sector actors further enable the reach of these operations. In this sense, SDIOs function as hybrid authoritarian instruments, blending the tools of soft power with coercive digital repression.

Our investigation also highlights the targeting of foreign journalists, academics, and politicians who voice criticism of Indian or Turkish state policies. These actors are often smeared, surveilled, or accused of "anti-national" sympathies, fostering a climate of fear, mistrust, and self-censorship. Through the widespread use of social media tracking, digital harassment, and orchestrated disinformation campaigns, critics are delegitimised and rendered suspect – sometimes even labeled as "terrorists" or "traitors." Such rhetoric has been internalised by supporters of the ruling parties in both countries, contributing to a toxic political culture that normalises repression under the guise of protecting national unity and sovereignty.

This digital authoritarian model, rooted in nationalist and religious narratives, has far-reaching implications for democratic norms, civil society, and global freedom of expression. It does not merely suppress individual dissent; it reshapes the conditions under which dissent, dialogue, and democratic engagement are possible. In both India and Turkey, fervent support for the regime is cultivated through the systematic blending of ideology, technology, and transnational mobilisation.

Funding: This work was supported by Australian Research Council [Grant Number DP230100257]; Gerda Henkel Foundation [Grant Number AZ 01/TG/21]; Australian Research Council [Grant Number DP220100829].

Note

1 See, for instance, https://www.youtube.com/watch?v=pMfmBo6rTuM&t=22s&ab_channel=Nchtuk

References

Abul, T., & Pyke, N. 2023. "Violent ethnic clashes in Leicester last year were stoked by Modi's Hindu nationalist party." *Daily Mail Online*. Retrieved November 10, 2023, from https://www.dailymail.co.uk/news/article-12081129/Violent-ethnic-clashes-Leicester-year-stoked-Modis-Hindu-nationalist-party.html

Adamson, F., & Tsourapas, G. 2020. At home and abroad: Coercion-by-proxy as a tool of transnational repression. In *Perspectives on 'Everyday' Transnational Repression in an Age of Globalization*. Freedom House, Special Report, 9–13. https://freedomhouse.org/report/special-report/2020/perspectives-everyday-transnational-repression-age-globalization

Al Jazeera. 2016. "Travel warning for German MPs of Turkish origin." *Al Jazeera*, June 12.

Al Jazeera. 2023. "India blocks BBC documentary on Modi's role in Gujarat riots." *Al Jazeera News*, January 21. https://www.aljazeera.com/news/2023/1/21/india-asks-youtube-twitter-to-block-links-of-bbc-film-on-modi-gujarat-riots

Al Jazeera. 2024a. "Hate crime tracker Hindutva Watch blocked in India ahead of national vote." *Al Jazeera News*, January 31. https://www.aljazeera.com/news/2024/1/31/hate-crime-tracker-hindutva-watch-blocked-in-india-ahead-of-national-vote

Al Jazeera. 2024b. "India's demand to block accounts amid farmers' stir curtails free speech: X." *Al Jazeera News*, February 22. https://www.aljazeera.com/news/2024/2/22/indias-demand-to-block-accounts-amid-farmers-stir-curtails-free-speech-x

Al-Khalaf, L. 2023. "How the far right fanned the flames in Leicester." *The Times (UK)*, September 26. https://www.thetimes.co.uk/article/how-the-far-right-fanned-the-flames-in-leicester-sljw8zjht

Aotearoa Alliance of Progressive Indians. 2021. "Why is the High Commission of India in Aotearoa spreading disinformation?" *AAPI Blog*, October 29. Retrieved November 9, 2023, from https://www.aotearoaprogressiveindians.org/_why_is_the_high_commission_of_india_in_aotearoa_spreading_disinformation

Arshad, M. 2023. "Unmasking Hinduphobia in the US." *Harvard Political Review*. Retrieved November 9, 2023, from https://harvardpolitics.com/unmasking-hinduphobia-in-the-us/

Associated Press. 2017. "Erdogan urges Turks in Europe to have 5 children." *AP News*, March 17.

Audrey Truschke. *Hindu Right in the United States*. Retrieved November 12, 2023, from https://www.audreytruschke.com/hindu-right-us-oxford-research-encyclopedia.

Australian Hindu Media [@austhindu]. n.d.a. "Tweet (with images) highlighting protest against ABC News coverage, posted June 19, 2024." *Twitter*. https://twitter.com/austhindu/status/1769198336714887525

Australian Hindu Media [@austhindu]. n.d.b. "With @ABCaustralia producing an incessant stream of stories perceived to be biased against Hindus & India, a mock protest was held in Melbourne today to highlight this portrayal by @ABC.Mosiqi Acharya heads ABC News's Asia Pacific Newsroom; Avani Dias is its India correspondent. Https://t.co/Vnef3iAQd7 [Tweet]." *Twitter*. Retrieved June 19, 2024, from https://twitter.com/austhindu/status/1769198336714887525/photo/2

Banaji, S., Bhat, R., Agarwal, A., Passanha, N., & Pravin, M. S. 2019. *WhatsApp Vigilantes: An Exploration of Citizen Reception and Circulation of WhatsApp Misinformation Linked to Mob Violence in India*. London: London School of

Economics. https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/WhatsApp-Misinformation-Report.pdf
Beauchamp, Z. 2024. "'Everyone is absolutely terrified': Inside a US ally's secret war on its American critics." *Vox*, May 22. https://www.vox.com/world-politics/24160779/inside-indias-secret-campaign-to-threaten-and-harass-americans
Bellut, D. 2021. "Turkish government increases pressure on social media." *DW*, September 9. https://www.dw.com/en/turkish-government-increases-pressure-on-social-media/a-59134848
Bianet, E. 2020. "There are 54 million social media users in Turkey." *Bianet*, July 2. https://m.bianet.org/english/society/226764-there-are-54-million-social-media-users-in-turkey
BJP [@BJP4India]. 2023. "Puppet in the hand of foreign powers . . ." (social media post depicting George Soros and opposition leader Rahul Gandhi), *Twitter/X*, October 6. https://twitter.com/BJP4India/status/1710203556370976840
Bozkurt, Abdullah. 2020. *Turkey Interrupted: Derailing Democracy*. Stockholm: Nordic Research and Monitoring Network.
Bulut, E., & Yörük, E. 2017. "Digital populism: Trolls and political polarization of Twitter in Turkey." *International Journal of Communication* 11, 4093–4117.
Canada Asia Pacific Foundation (CAST). 2023. "Sensationalist headlines dominate Indian media's coverage of assassination allegations." *Event Brief*. Retrieved November 11, 2023. https://cast.asiapacific.ca/map/event/4138
Chandran, R. 2021. "'Like the Stasi': India's cyber volunteers silence critical voices." *Sydney Morning Herald*, December 1. https://www.smh.com.au/world/asia/like-the-stasi-india-s-cyber-volunteers-silence-critical-voices-20211129-p59d41.html
Chaudhuri, P. 2020. "Amit Malviya's fake news fountain: 16 pieces of misinformation spread by the BJP IT cell chief." *Scroll.in*, February 10. https://scroll.in/article/952731/amit-malviyas-fake-news-fountain-16-pieces-of-misinformation-spread-by-the-bjp-it-cell-chief
Citizens and Lawyers Initiative. 2020. *Delhi Riots 2020: Causes, Fallout and Aftermath*. https://drive.google.com/file/d/1gOw2XXuR2whrZGy3P-XeVf-CEHbi1Mty/view
Connolly, Kate. 2016. "German parliament condemns threats to MPs after Armenian vote." *The Guardian*, June 9.
Dasgupta, S. 2023. "Why India is awash with anti-Palestine disinformation." *Coda Story (Disinformation Matters newsletter)*, November 9. https://www.codastory.com/newsletters/india-hindu-nationalism-gaza/
DFR Lab (Digital Forensic Research Lab). 2019. "#ElectionWatch: Inauthentic activity in India." *Medium (DFRLab)*, April 1. https://medium.com/dfrlab/electionwatch-inauthentic-activity-in-india-8940588e09b5
The Economic Times. 2024. "'Modi for 2024': Overseas friends of BJP, Australia launches campaign to drum up support ahead of LS polls." *Economic Times*. https://economictimes.indiatimes.com/news/elections/lok-sabha/india/modi-for-2024-overseas-friends-of-bjp-australia-launches-campaign-to-drum-up-support-ahead-of-ls-polls/articleshow/108748804.cms
Ellis-Petersen, H. 2021. "Death threats sent to participants of US conference on Hindu nationalism." *The Guardian*, September 9. https://www.theguardian.com/world/2021/sep/09/death-threats-sent-to-participants-of-us-conference-on-hindu-nationalism
Elmas, T., Overdorf, R., Özkalay, A., & Aberer, K. 2019. *Ephemeral Astroturfing Attacks: The Case of Fake Twitter Trends*. https://www.researchgate.net/publication/336638958_Ephemeral_Astroturfing_Attacks_The_Case_of_Fake_Twitter_Trends
Financial Express. 2020. "Over 100,000 Indian-Americans watch virtual Hindus4Trump rally." *The Financial Express (India)*, August. https://www.

financialexpress.com/world-news/over-100000-indian-americans-watch-virtual-hindus4trump-rally/2029292/
Freedom House. 2021. *Freedom on the Net 2020 – Turkey*. Report. https://freedomhouse.org/country/turkey/freedom-net/2020
Freedom House. 2022. *Defending Democracy in Exile: Policy Responses to Transnational Repression*. Washington, DC: Freedom House.
Freedom House. 2023. *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*. Global Report, especially country chapter on India, October. https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf
Friedrich, P. 2024. "Highlights reel of Hindutva interference in US sociopolitics." *Medium*, February 8. https://pieterjfriedrich.medium.com/highlights-reel-of-hindutva-interference-in-us-sociopolitics-4c501762decc
Grossman, S., Tianshi, E., Thiel, D., & DiResta, R. 2022. *My Heart Belongs to Kashmir: An Analysis of a Pro-Indian Army Covert Influence Operation on Twitter*. Stanford: Stanford Internet Observatory.
Hacaoglu, Selcan. 2020. "France bans Turkish ultra-nationalist group gray wolves." *Bloomberg*, November 2.
Harper, Jon. 2020. "Twitter removes network of fake accounts pushing pro-Erdoğan propaganda." *Stars and Stripes*, June 12.
Human Rights Watch. 2020. *Turkey Events of 2020*. https://www.hrw.org/world-report/2021/country-chapters/turkey
Hundal, S. 2019. "The anti-labour plot to polarise Hindus over Kashmir." *openDemocracy UK*, November 7. https://www.opendemocracy.net/en/opendemocracyuk/anti-labour-plot-polarise-hindus-over-kashmir/
Hussain, M., & Grim, R. 2023. "Secret Indian memo ordered 'concrete measures' against Hardeep Singh Nijjar two months before his assassination in Canada." *The Intercept*, December 10. https://theintercept.com/2023/12/10/india-sikhs-leaked-memo-us-canada/
India Today. 2024. "Canada says India second-biggest foreign threat to its democracy after China: Report." *India Today (Online)*, June 6. https://www.indiatoday.in/world/canada-news/story/justin-trudeau-canada-india-second-biggest-foreign-threat-democracy-china-russia-report-nsicop-khalistani-2549826-2024-06-06
Indian Century Roundtable. n.d. *Website of an NRI Group Supportive of Modi*. Retrieved June 19, 2024, from https://www.indiancentury.org/
Infinity Foundation Official (Rajiv Malhotra's Channel). n.d. YouTube Channel. Retrieved June 20, 2024, from https://www.youtube.com/@RajivMalhotraOfficial
Jenkins, Gareth. 2018. "Erdoğan's expanding global purge." *The Turkey Analyst* 11(8).
Johal, R. 2023. "A new wave of online harassment and misinformation campaigns are targeting Sikhs in Canada." *PressProgress (Canada)*, April 6. https://pressprogress.ca/a-new-wave-of-online-harassment-and-misinformation-campaigns-are-targeting-sikhs-in-canada/
Johal, R. 2024. "Intelligence report says bots and fake accounts linked to India's governing party are harassing Canadians." *PressProgress*, April 6. https://pressprogress.ca/intelligence-report-says-bots-and-fake-accounts-linked-to-indias-governing-party-are-harassing-canadians/
Jones, M. O. 2022. *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. Hurst Publishers.
Karan, Taha. 2020. "How Turkey's diaspora uses WhatsApp to shape politics back home." *BBC Turkish* (online), May 5.
Karanicolas, M. 2021. "Authoritarianism as a service: India's moves to weaponize private sector content moderation with the 2021 information technology rules." *Indian Journal of Law and Technology* 17(2), 4.

Legrello, Luca. 2021. "Turkish influence in Europe: The three-tier strategy." *FEUTURE Working Paper*.
Livemint. 2024. "Overseas friends of BJP holds a 250-car rally in London to show support for PM Modi ahead of Lok Sabha elections." *Livemint*, March 18. https://www.livemint.com/news/india/uk-overseas-friends-of-bjp-holds-car-rally-to-support-pm-modi-for-upcoming-elections–11710723119382.html
Machado, G., Alaphilippe, A., Adamczyk, R., & Grégoire, A. 2019. *Indian Chronicles: Subsequent Deep Dive into a 15-Year Operation Targeting the EU and UN to Serve Indian Interests*. EU DisinfoLab Report. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/
Maritato, C. 2021. "Pastors of a dispersed flock: Diyanet officers and Turkey's art of governing its diaspora." *Italian Political Science Review/Rivista Italiana Di Scienza Politica* 51(3), 321–338. https://doi.org/10.1017/ipo.2020.31
Mathew, N. 2022. "Bhakt nation: The return of the Hindu diaspora in Modi's India." *History and Anthropology* 33(3), 337–354. https://doi.org/10.1080/02757206.2021.1946049
Mehrotra, K., & Menn, J. 2023. "How India tamed Twitter and set a global standard for online censorship." *The Washington Post*, November 8. https://www.washingtonpost.com/world/2023/11/08/india-twitter-online-censorship/
Merhi, M., Rajtmajer, S., & Lee, D. 2023. Information operations in Turkey: Manufacturing resilience with fake Twitter accounts. *Proceedings of the 17th International AAAI Conference on Web and Social Media (ICWSM 2023)*, 638.
Michaelsen, M. 2020. "The digital transnational repression toolkit and its silencing effects." In *Perspectives on 'Everyday' Transnational Repression in an Age of Globalization*. Freedom House, Special Report, 4–8. https://freedomhouse.org/report/special-report/2020/perspectives-everyday-transnational-repression-age-globalization
Mihindukulasuriya, R. 2021. "These are the apps and websites Modi Govt blocked in 2020." *ThePrint*, March 18. https://theprint.in/india/governance/these-are-the-apps-and-websites-modi-govt-blocked-in-2020/623337/
Naik, R. H. 2021. "'US academic conference on 'Hindutva' targeted by Hindu groups'." *Al Jazeera*, September 7. https://www.aljazeera.com/news/2021/9/7/us-academic-conference-dismantling-global-hindutva-hindu-right-wing-groups
Newsroom (NZ). 2021. "Indian diplomats weigh in on academic spat." *Newsroom.co.nz*, April 14. https://www.newsroom.co.nz/pro/indian-diplomats-weigh-in-on-hindutva-spat
Niranjankumar, N. 2022. "How Indian High Commission – and media – falsely claimed a 'Hate Crime' Happened at a Canada Park." *The Wire*, October 4. https://thewire.in/media/fact-check-brampton-canada-park-hate-crime-vandalise
NT, S. (Medianama). 2024. "Indian govt blocks YouTube satire video by the Juice Media." *Medianama*, June 13. https://www.medianama.com/2024/06/223-indian-govt-blocks-youtube-satire-video-juice-media/
Öktem, Kerem. 2014. *Turkey's New Diaspora Policy: The Challenge of Inclusivity, Outreach and Capacity*. Istanbul Policy Center Report.
Pahwa, N. 2020. "The Hindu nationalist Trump supporters taking over WhatsApp." *Slate*, October 28, 2020. https://slate.com/news-and-politics/2020/10/trump-whatsapp-hindu-nationalism-modi.html
Patel, J., & Chaudhuri, J. 2019. "'The India Eye' – the fake news factory promoted by NaMo app." *The Wire (India)*, February 7. https://thewire.in/media/the-indian-eye-fake-news-factory-namo-app-silver-touch
Punit, I. S. 2016. "Hindu groups in California oppose the proposed revisions to school textbooks." *Quartz India*, April 1. https://qz.com/india/666103/hindu-groups-in-california-oppose-the-proposed-revisions-to-school-textbooks

Rediff.com. 2024. "Western media's coverage of Ram Mandir biased: VHP." *Rediff News*, January 24. https://www.rediff.com/news/report/western-medias-coverage-of-ram-mandir-biased-vhp/20240124.htm

Reuters. 2017. "Twitter accounts hijacked with 'Nazi' hashtags in Turkish." *Reuters*, March 15. https://www.reuters.com/article/us-cyber-turkey-idUSKBN16M11J

Ruijgrok, K. 2022. "The authoritarian practice of issuing internet shutdowns in India: The BJP's direct and indirect responsibility." *Democratization* 29(4), 611–633.

Saka, E. 2018. "Social media in Turkey as a space for political battles: AKTrolls and other politically motivated trolling." *Middle East Critique* 27(2), 161–177. https://doi.org/10.1080/19436149.2018.1439271

Schenkkan, N. 2020a. Introduction. In *Perspectives on 'Everyday' Transnational Repression in an Age of Globalization*, Freedom House, Special Report, 1–3. https://freedomhouse.org/report/special-report/2020/perspectives-everyday-transnational-repression-age-globalization

Schenkkan, Nate. 2020b. "Turkey's transnational repression." *The Washington Post*, September 21.

Scroll. 2023. "X accounts of Indian American Muslim Council, Hindus for Human Rights withheld in India." *Scroll.in*, October 31. https://scroll.in/latest/1057702/x-accounts-of-indian-american-muslim-council-hindus-for-human-rights-withheld-in-india

Scroll. 2024. "YouTube, X block access in India to documentary on killing of Canadian Sikh separatist leader." *Scroll.in*, March 14. https://scroll.in/latest/1065190/youtube-x-block-access-to-documentary-on-killing-of-canadian-sikh-separatist-leader-in-india

Shakir, Kevin, et al. 2023. "Leaked documents reveal Russian fake protests to provoke Erdoğan." *Dossier Center/DR (investigative project)*, May 7.

Sharma, Y. 2023. "Twitter accused of censorship in India as it blocks Modi critics." *The Guardian*, April 5. https://www.theguardian.com/world/2023/apr/05/twitter-accused-of-censorship-in-india-as-it-blocks-modi-critics-elon-musk

Shih, G. 2023. "Inside the vast digital campaign by Hindu nationalists to inflame India." *Washington Post*, April 26. https://www.washingtonpost.com/world/2023/09/26/hindu-nationalist-social-media-hate-campaign/.

Shih, G., Ence Morse, C., & Verma, P. 2023. "Covert Indian operation seeks to discredit Modi's critics in the U.S." *Washington Post*, December 11. https://www.washingtonpost.com/world/2023/12/10/india-the-disinfo-lab-discredit-critics/

Sign the Petition. 2023. *Change.Org*. Retrieved June 20, 2024, from https://www.change.org/p/stop-deakin-university-from-encouraging-hindu-phobia

Strick, B. 2022. "Analysis of the #RealSikh influence operation." *Centre for Information Resilience*. https://www.info-res.org/post/revealed-real-sikh-influence-network-pushing-indian-nationalism

Swyers, K., & Trinh, J. 2022. "Hate speech and death threats: Canadian academics harassed after criticizing Hindu nationalism in India." *CBC News (Canada)*, April 7. https://www.cbc.ca/news/canada/academics-harassed-criticism-india-politics–1.6402486

Taş, Hakkı. 2018. "The 2017 referendum in Turkey: Divide and rule." *Mediterranean Politics* 23(3), 393–400.

Twitter Safety. 2020. "Disclosing networks of state-linked information operations we've removed." *Twitter Official Blog*, June 12. https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020

van der Noordaa, Wouter. 2020. "Dutch court convicts erdoğan supporter for threatening journalist." *De Telegraaf (Netherlands)*, February 10.

VHP America [@VHPANews]. 2024. *Tweet with Images Promoting Ram Mandir Event*, January 14. https://x.com/VHPANews/status/1793503224777068644

Wilson, A. 2017. "Why is the UK government wheeling back on legislation against caste discrimination?" *openDemocracy UK*, October. https://www.opendemocracy.net/en/opendemocracyuk/why-is-uk-government-wheeling-back-on-legislation-against-caste-discrimination/

The Wire. 2022. "'We support Canada's investigation . . . into this terrible assassination', says senior US official." *The Wire (India)*, November. https://thewire.in/world/india-canada-us

The Wire. 2023a. "Over 55,000 websites blocked since January 2015, most to 'protect Indian state': Report." *The Wire*, January 17. https://thewire.in/tech/over-55000-websites-blocked-since-january-2015-most-to-protect-indian-state-report

The Wire. 2023b. "How Indian High Commission – and media – falsely claimed a 'hate crime' happened at a Canada park." *The Wire*, March. https://thewire.in/media/fact-check-brampton-canada-park-hate-crime-vandalise

The Wire. 2024a. "As India blocks 'Honest Government' YouTube short, Australian creator says he was guided by Indians." *The Wire*, June 21. https://thewire.in/rights/honest-government-ad-youtube-short-video-blocked-india

The Wire. 2024b. "US State Dept accuses India of anti-Semitism for pushing conspiracies against George Soros." *The Wire*. Retrieved June 20, 2024, from https://thewire.in/government/us-state-dept-accuses-india-of-anti-semitism-for-pushing-conspiracies-against-george-soros

Yeşil, Bilge. 2024. *Talking Back to the West: How Turkey Uses Counter-Hegemony to Reshape the Global Communication Order*. Champaign, IL: University of Illinois Press.

Yilmaz, I., Akbarzadeh, S., & Bashirov, G. 2023. *Strategic Digital Disinformation Operations (SDIOs)*. European Center for Populism Studies (ECPS). Retrieved November 12, 2023, from https://www.populismstudies.org/comprehending-the-tactics-of-strategic-digital-disinformation-operations-sdios/

Yilmaz, I., & Shipoli, E. 2022. "Use of past collective traumas, fear and conspiracy theories for securitisation and repression of the opposition: The Turkish case." *Democratization* 29(2), 320–336. https://doi.org/10.1080/13510347.2021.1953992

York, Jillian. 2020. "Twitter's decision to Ban Turkish accounts is a wake-up call." *Foreign Policy*, June 19.

Zhang, A. 2022. "Inauthentic accounts increasingly shaping South Asian social media." *The Strategist (ASPI)*, August 31. https://www.aspistrategist.org.au/inauthentic-accounts-increasingly-shaping-south-asian-social-media/

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

PART 5

Non-State Actors and Extremism

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

13

DIFFERENCES IN THE UTILISATION OF DIGITAL TOOLS FOR INFORMATION OPERATIONS BETWEEN STATE AND NON-STATE ACTORS

Mohamed Ibrahim

Introduction

The chapter introduces the reader to the concept of IO in the digital age. It will explain the relevance of this topic in the current global terrain, where digital platforms have immense power in shaping public perception. This is especially relevant in today's digitally driven world where both state and non-state actors use social media to significantly impact political, social, and economic narratives.

As researchers in the field have pointed out in what they have described as SDIOs (Yilmaz et al. 2023), the impact of this phenomenon has been felt in both national and international contexts, targeting domestic and foreign audiences through an array of tactics to achieve the political goals of their organisers. This has direct implications on the functioning of both national governments and international entities. The danger is what their influences can do to the legal mechanism in place for social, financial, and political institutions.

While the objectives of both sets of actors, that is, state and non-state to pursue their political goals may seem similar, there are certain differences in the methods employed resources available to them. The state actors tend to be well resourced and possess good infrastructure of human and technological capital. They tend to have access to a range of digital tools to be used in domestic and foreign contexts, whether to silence the critics and legitimise their rule at home or destabilise their adversaries and extend their geopolitical influence abroad. They tend to carefully plan campaigns to infiltrate foreign information systems, reshape stories, and generate social conflicts, all of which take long-term thinking and strategic foresight. On the other hand,

DOI: 10.4324/9781003628088-18
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

non-state actors, including hacktivist groups and extremist organisations, may lack resources but they tend to be more adaptable to new environments. Ordoñez de Pablos (2023) has pointed out that they use digital platforms to promote their causes, attract supporters, and amplify their voices. These players maneuver through the digital world with agility, reflecting the changing nature of the medium.

The chapter is structured as follows. The introduction will be followed by the background section which will provide context to the key issues discussed. The next four sections will cover understanding information operation by navigating the digital age, and its relevance in global terrain, and how this impacts democracy and governance from global security and geopolitical dynamic perspective. A case study on Somali government and Alshabab will be followed by the Discussion and Conclusion section.

Background

This chapter will outline the primary differences between state and non-state actors in terms of their resources, objectives, and methodologies in using digital tools for IO. This can include examples of how each group typically operates in the digital space. Incorporating case studies and real-world examples to illustrate how state and non-state actors have utilised digital tools in recent history which will involve analysis of specific social media campaigns, cyber operations, or digital propaganda efforts.

The methodological approach used in understanding this field is qualitative and in-depth literature review. The focus being on the implications of the utilisation of digital tools for IO by state and non-state actors affects the functioning of national governments, financial institutions, and the global security. It will address the changing terrain of digital information warfare and its implications for international relations, public trust, and governance.

The chapter presents a comprehensive methodological framework for analyzing the differential use of digital tools in IO by state and non-state actors. Recognising the complex nature of digital information warfare, the emphasis will be the need for deeper understanding and approaches to capture the multifaceted strategies employed by these actors to enhance our understanding of the digital information terrain and its implications for global security.

The previous objective will be achieved by contextualising the importance of IO in the digital age and the challenges in researching the diverse strategies state and non-state actors use, for example, as Perloff (2021) pointed out that authoritarian governments employ tactics such as digital censorship and in some cases surveillance methods to suppress dissenting voices and exert control over digital narratives, while in other cases such as used by populist leaders, might be harnessing the immediacy and interactive nature of social media to establish direct, emotional connections with their constituents, bypassing

traditional gatekeepers. By capitalising on the resonance of online platforms, these actors perpetuate narratives that exploit societal grievances, positioning themselves as advocates for the marginalised while vilifying opposing viewpoints (Postill 2018).

Studies attempting to explain how IO have been within the social media context have identified sophisticated technical tools used for manipulations within the platforms to distort views and ideas to misinform consumers of their content (Starbird et al. 2019). Even major social media platforms such as X (formerly Twitter) and Meta (formerly Facebook) were found to spread dis/misinformation via usage of certain pieces of information that resonate with users and generate an expected response, such as those that are more surreal, exaggerated, impressive, emotional, persuasive, clickbait, and shocking images tend to generate better results (Yilmaz et al. 2023).

Starbird et al. (2019) also use the term strategic IO to refer to efforts by individuals and groups, including state and non-state actors, to manipulate public opinion and change how people perceive events in the world by intentionally altering the information environment. Tracing their roots to TV and radio propaganda in the 20th century, and in some variation even much earlier (Posetti & Matthews 2018), the modern digital age and in particular today's social media terrain have enabled these efforts with unparalleled efficiency and have raised a unique set of questions around IO which aims to disseminate inaccurate, incorrect, or misleading information or disinformation.

Abuse of IO can have serious implication as (Benkler et al. 2018) reminded us in critical example for the US, when Russian IO around the 2016 Presidential Elections targeted key political institutions such as the political parties, the Congress, and the Constitutional Court through hacking, manipulative messaging, and social media campaigns, leading to erosion of trust among American citizens on these institutions.

In the contemporary terrain of global communication, the advent of the digital age has revolutionised the way information is disseminated and consumed. At the intersection of this transformation lies the concept of IO, a field that has gained prominence due to its profound impact on public perception and, subsequently, on political, social, and economic paradigms. IO refer to the strategic use of information to influence, disrupt, corrupt, or usurp the decision-making process of adversaries while protecting our own (Rajtmajer & Susser 2020). In the digital age, these operations leverage the vast reach and immediacy of digital platforms, including social media, online news outlets, and various internet-based communication tools. This chapter aims to introduce readers to the nuances of IO in the digital age, underlining its significance in the current global terrain shaped by digital platforms.

The digital age has ushered in an era where information is not just a resource but a weapon that can be used to attack different social and economic sectors of the society. The rapid proliferation of digital platforms,

including social media, online forums, and various other internet-based communication channels, has provided fertile ground for the execution of sophisticated IO. Unlike traditional modes of communication, digital platforms facilitate instantaneous, widespread dissemination of information, transcending geographical boundaries and impacting a global audience (Waltzman 2017).

To effectively discuss the differences in the utilisation of digital tools for IO between state and non-state actors, it is essential to clearly define the key terms involved in this analysis:

Information Operations: IO refer to activities conducted by organisations or individuals to influence, disrupt, corrupt, or usurp the decision-making of adversaries or competitors while protecting their own. In the digital age, this often involves the use of cyber tools and tactics to manipulate information, spread propaganda, or disrupt communication. IO can encompass a broad range of activities, including psychological operations, cyber operations, electronic warfare, and influence campaigns.

Digital Tools: In the context of information, operations include a wide array of technologies and platforms used to conduct cyber activities. These can range from basic tools like social media platforms, websites, and forums, to more sophisticated technologies such as malware, hacking tools, bots, and artificial intelligence algorithms. These tools are used to disseminate information, manipulate data, conduct surveillance, or interfere with digital infrastructure.

State Actors: It refers to governments and their affiliated organisations, including intelligence agencies, military units, and other governmental entities. In IO, state actors typically have significant resources and capabilities, allowing them to engage in complex and sophisticated operations. Their activities can be aimed at both domestic and international audiences and can involve objectives like national security, political control, or international influence.

Non-State Actors: They include a wide range of entities that are not directly tied to any government. This category can include terrorist groups, activist networks, private corporations, non-governmental organisations (NGOs), and even individual hackers or hacktivist groups. Non-state actors may have varying levels of resources and capabilities. Their motives for engaging in IO can range from political and social causes to financial gain or personal beliefs.

Differentiating between criminal hackers and nation-state actors complicates what was traditionally called defense strategies. Some nations provide safe havens to criminal hackers, further blurring the lines between state and non-state cyber threats. Therefore, understanding these key terms helps frame

the analysis of how different actors leverage digital tools in the realm of IO, revealing their varying capabilities, objectives, and methods.

Both state and non-state actors can often engage in coordinated IO across borders, leveraging social media platforms for cheap and easy content dissemination, profiling, and targeting. These operations often involve ambient affiliation through common hashtags, network expansion for increased exposure, and referencing controversial topics to attract attention. Strategic IO by states manipulate public opinion by altering the information environment, a practice tracing its roots to early 20th-century propaganda (CSIS 2022).

The utilisation of digital tools for IO varies significantly between state and non-state actors. This difference can be observed in various aspects such as tactics, strategies, goals, and the nature of their operations.

State Actors

State actors use IO strategically to influence populations and governments. These operations are diverse, including military information support, psychological operations, and disinformation campaigns. Information warfare declines, and revival was noticed after the cold war in the US which allowed its information warfare capabilities to decline. Only recently, with the rising threat from state actors like Russia and China, has there been a renewed focus on enhancing these capabilities (De Poli 2017).

Countries like China and Russia invest significantly in controlling information environments. Russia spends about $1.3 billion annually on strategic communications, while China exceeds $10 billion, in addition to their disinformation operations. However, there is a need for a law enforcement collaboration in this area for all nations to defend against cyber threats, particularly those motivated by financial gains like ransomware attacks.

State actors, especially those backed by considerable resources, have shown a propensity for engaging in sophisticated and coordinated strategic IO. These operations often involve collaboration across states and are marked by a high degree of organisation and strategic interaction. For instance, a study analyzing Twitter data between 2011 and 2021 revealed that state-backed campaigns demonstrated greater engagement and impact than intra-state operations (Wang et al. 2023). They employed tactics like ambient affiliation through common hashtags, network expansion, and referencing controversial topics to garner attention.

State actors utilise social media platforms extensively due to their reach and the ease of content dissemination. These platforms enable the propagation of disinformation, often associated with political campaigns and social media manipulation through bot accounts and paid workers. The primary aim is often to disseminate inaccurate or misleading information to shape public opinion and perceptions.

The involvement of state actors in cyberspace is not just limited to information warfare but extends to cyber warfare. States often contract non-state actors due to limited resources or expertise in this domain. These non-state actors, while not directly a part of the state apparatus, help in achieving the state's political, military, and commercial goals, often engaging in espionage, propaganda, disruption, sabotage, and retaliation against adversaries.

Non-State Actors

Non-state actors in cyberspace include individuals, groups, or organisations that operate independently or in association, often without specific physical territory or territorial sovereignty. These actors find cyberspace an ideal ground due to low entry barriers and high anonymity. Their operations range from hostile acts to promoting geopolitical and geoeconomic rivalries, with little to no immediate consequences due to the difficulty in attributing these actions to specific entities.

Non-state actors often engage in SDIOs, which involve manipulating public opinion and emotions using digital technologies. These operations significantly influence societal issues like emotive political mobilisation, intergroup relations, social cohesion, trust, and emotional resonance among target audiences (Yilmaz et al. 2023).

Recently, there has been a shift in the tactics of non-state actors from blatant disinformation to more sophisticated means of manipulation. This change is in response to the growing awareness and clampdown on fake news by digital platforms and users. The new tactics include spreading half-truths, investing in smart public relations messages, and flooding the information space with distracting and irrelevant information, often with the help of trolls, bots, social media consultants, influencers, and genuine followers.

The literature also reveals powerful non-state groups that perform proxy operations and often operate on behalf of states, offering plausible deniability to these nations. Examples include The Concord Group in Russia, which owns the Internet Research Agency known for disinformation campaigns. These independent actors and criminal groups are not necessarily advanced persistent threats but pose significant cyber threats, primarily financial. Ransomware operations by such groups can generate millions in profit, targeting industries with weaker cyber defenses like academia, healthcare, and smaller government entities. These non-state armed groups do not pose a significant cyber threat to nations like the US and its allies currently, except when acting as state proxies. Developing cyberattack capabilities requires a different skillset than that needed for kinetic attacks.

Non-state actors are increasingly accessing capabilities once reserved for state actors, often available on the dark web. This democratisation of cyber tools has leveled the playing field, making non-state actors more formidable.

While state actors traditionally engage in more sophisticated, high-impact operations, non-state actors' motivations and strategies are more varied and less predictable. They often engage in cyber operations for financial gain, while state actors tend to have broader strategic and geopolitical objectives.

Within the non-state actors, there are cyberspace native groups, who are organisations native to cyberspace, like hacking collectives and ransomware groups, that have significantly impacted geopolitics through cyber operations. These groups, including those with histories rooted in kinetic violence, are adopting offensive cyber capabilities to further their strategic objectives, such as the Wagner Group in Russia and various militant organisations like Hezbollah and Boko Haram.

The low barriers to acquiring and deploying offensive cyber tools indicate a growing cyber capacity among non-state armed groups. These groups are driven by a range of motivations including financial gains, ideological causes, or even just for fun, making their actions highly unpredictable and challenging to defend against. While non-state actors are becoming more capable in the digital realm, often with financial motives, state actors continue to lead in strategic influence and investment in IO. The complexity and dynamism of the cyber domain necessitate continual evolution in defense and offensive strategies for both state and non-state actors (Pearlman 2019).

Relevance in the Global Landscape

The relevance of IO in today's world cannot be overstated. In a terrain where public opinion can be significantly swayed by online content, the ability to manipulate this content becomes a powerful tool. State actors, non-state actors, and even individuals have harnessed the capabilities of digital tools to advance their agendas, be it for political gain, social influence, or economic advantage. The Cambridge Analytica scandal, for instance, highlighted how personal data can be exploited for political advertising, influencing voter behavior (Cadwalladr & Graham-Harrison 2018). Such incidents underscore the potency of IO in shaping political terrains and public opinion.

The strategies employed in digital information warfare present complex challenges for global security, international relations, public trust, and governance. As technology continues to evolve, so too must the strategies to combat these threats. This involves not just technological solutions but also a rethinking of legal, ethical, and policy frameworks on a global scale. The need for international cooperation and robust cybersecurity measures has never been more critical in this digital age. The impact of digital strategies on global security, particularly in the context of digital information warfare, international relations, public trust, and governance, is multifaceted and complex.

The utilisation of digital tools for IO by state and non-state actors has evolved significantly, particularly in the realm of social media and cyber operations. The differences in their approaches, capabilities, and objectives offer a complex view of contemporary geopolitical strategies in the digital domain.

Beyond influencing public opinion, IO have become a strategic element in national security and global politics. Nations engage in cyber operations not only to defend their own digital infrastructure but also to project power, influence adversaries, and shape geopolitical narratives. This new battleground, where information is both shield and sword, has redefined the contours of international relations and security paradigms. The Stuxnet cyberattack on Iranian nuclear facilities is a prime example of how digital tools can be used for strategic geopolitical objectives (Langner 2011).

A new assertion in the literature from (Yilmaz et al. 2023) has introduced the emergence of "sharp power" which has been denoted as a significant shift in the way global interactions are conducted. This has influenced the dynamics of external influence, as digital platforms have become tools that are being used to influence decisions that impact relations between countries such as the US, China, and Russia, as well as middle powers such as Australia, Türkiye, and Egypt. For example, over the last decade, Australia, its public authorities, media entities, and civil society organisations have been systematically targeted by Chinese sharp power operations that included lavish donations to campaigns of useful political candidates, harassment of journalists, and spying on Chinese students in university campuses (The Economist 2017).

Political Parties as Non-State Actors

Non-state actors have increasingly played significant roles in shaping political terrains and influencing electoral outcomes across the globe. While traditionally, the term "non-state actors" might evoke images of NGOs, multinational corporations, or even terrorist groups, in the contemporary political context, it encompasses a wider range of entities, including political parties (when they are not in power), troll farms, and various advocacy groups. These actors, through diverse means, significantly impact elections and the democratic process.

When not in power, political parties operate as non-state actors, playing a crucial role in the democratic process. They mobilise support, articulate public demands, and influence policy by participating in elections. Their strategies include campaigning, policy development, and engaging with the electorate through traditional and digital platforms. Political parties, especially in countries with robust democratic institutions, contribute to the political discourse, offering choices to voters and ensuring that the governing parties are held accountable.

Troll farms represent a darker side of the influence exerted by non-state actors on elections. These are organised groups that use social media and other online platforms to spread misinformation, sow discord, and manipulate public opinion. Troll farms are often associated with state actors but operate in the shadows, allowing plausible deniability. Their tactics include creating fake accounts, disseminating false or misleading information, and amplifying divisive issues. By influencing what people see online, troll farms can sway public opinion, polarise societies, and even affect the outcomes of elections.

The activities of non-state actors such as political parties and troll farms can have profound effects on elections and the broader democratic process. Influence on voter behavior through targeted campaigns and misinformation, these actors can significantly influence voter behavior. Political parties aim to mobilise voters through persuasive messaging and policy proposals, while troll farms may attempt to demobilise or mislead voters, undermining the integrity of the electoral process.

Both political parties and troll farms can contribute to the polarisation of society. While political parties might do so as a by-product of promoting their ideologies, troll farms intentionally exploit societal divisions, exacerbating tensions and undermining social cohesion. Political parties, through their electoral success, directly influence policy. Their platforms and promises can shape national agendas and priorities. In contrast, troll farms indirectly influence policy by shaping the narratives and discussions around key issues, potentially diverting attention from substantive policy debates.

The actions of these non-state actors can either bolster or erode trust in the democratic process. Political parties, through constructive engagement and adherence to democratic norms, can strengthen democracy. However, the manipulative tactics of troll farms can erode trust in electoral processes, media, and the political discourse at large, posing a significant threat to democratic legitimacy. The role of non-state actors in elections is multifaceted and complex. While political parties are fundamental to the democratic process, offering a mechanism for representation and governance change, entities like troll farms represent a challenge to the integrity of elections. The influence of these actors underscores the need for robust democratic institutions, media literacy, and regulatory frameworks to safeguard the electoral process and ensure that democracy can thrive in the face of dynamic challenges.

The complex ecosystem of social media manipulation, where state and non-state actors collaborate and compete in shaping public discourse is widely discussed in the literature. The following summarises the main trends, focusing on the use of private contractors, volunteers, and paid citizens. While this highlights the interactions between agencies, organisations as well as government and private-sector groups, it is pertinent to keep in mind

that the boundaries are getting blurry and the linkages are overlapping and interconnected.

The use of private contractors highlights a strategic interface between governmental objectives and private-sector capabilities, exemplified by the US government's engagement with PR firms for persona management to craft online identities and the Internet Research Agency's efforts in Russia that align with Kremlin's digital influence campaigns. Volunteers also serve as a pivotal force in the spread of political ideologies, leveraging their enthusiasm and alignment with governmental goals. This is evident in Azerbaijan with youth organisations like IRELI and in Russia through Nashi, where indirect rewards such as scholarships in Israel motivate participation. The role of Paid Citizens in disseminating political messages under the guise of independent opinion reflects a complex approach to influence. This strategy is visible in India, where individuals' social stature is utilised to propagate political ideologies, enhancing message credibility through perceived neutrality.

To conclude, non-state actors, encompassing both political parties (when not in governmental power) and troll farms, play pivotal roles in influencing elections and shaping democratic processes. Political parties mobilise support and engage in policy development, contributing positively to the political discourse and offering voters distinct choices. In contrast, troll farms operate nefariously, spreading misinformation and manipulating public opinion online to sway electoral outcomes and polarise societies. These activities have significant implications for voter behavior, societal polarisation, policy influence, and the legitimacy of the democratic process. While political parties can reinforce democratic norms and processes through constructive engagement, the manipulative tactics of troll farms pose serious threats to the integrity and trust in electoral systems. Addressing these challenges requires strong democratic institutions, enhanced media literacy, and effective regulatory measures to protect the electoral process and ensure the resilience of democracy.

Shabab and Somali Government

A hybrid approach has been used to gauge how the Shabab uses the social media integrating network metrics and content-based analyses. Since October 2018, Twitter has made public the tweets, media, and account-related information of users presumed to be involved in state-linked IO, provided through the Twitter Moderation Research Consortium (TMRC). The TMRC suggests that these users are engaged in manipulation that can be reliably attributed to a government or state-linked actor.

Shabab, commonly referred to as "the youth," emerged in 2006 as an armed wing of the Islamic Courts Union (ICU), which has since become defunct. Despite the ICU's brief existence, Shabab persisted in its campaign across Somalia, aiming to implement a stringent version of Islamic law and

expel foreign entities. The group's objectives are widely considered unattainable and misguided for two main reasons. First, the influx of international aid, crucial for life sustenance in Somalia's impoverished and drought-stricken regions, is substantial. Somalia, a significant beneficiary of global aid with over $60 billion received since 1991, relies on these funds for humanitarian relief. However, a portion of this aid is misappropriated due to political instability and corruption (Hansen 2013). Shabab extensively uses media to spread propaganda and misinformation, utilising diverse platforms like web media (e.g., SomaliMemo, Shahada News), radio (e.g., Idaacadda Al Furqaan), and social media (e.g., Facebook, Twitter). Their media reach is expanding both physically and online, unimpeded. The obvious question authorities logically ask is why this terrorist group is allowed to register domain names and have access to social media platforms. This is beyond the scope of this chapter but be discussed in appendix to the chapter.

Furthermore, Shabab's involvement in criminal activities and terrorist acts against civilians and foreign targets necessitates the reinforcement of the Somali National Army (SNA) by foreign military forces under the African Union Mission in Somalia (AMISOM). Over 20,000 AMISOM troops, supported internationally, assist the SNA in counteracting Shabab. The SNA is often assessed as inadequately equipped and prepared to sustain security independently, highlighting the paradox of foreign presence being both a response to and a target of Shabab's violence, which often results in civilian casualties. Shabab also generates significant revenue through illegal taxation, extorting local businesses and exploiting remittances from the Somali diaspora. These funds support their operations and media endeavors. The group manipulates clan politics in Somalia, exacerbating internal divisions and exploiting them for gain. They use media, especially radio, to deepen tribal rifts and secure allegiances, often at the expense of social cohesion and safety. Shabab's connections with international terrorist networks, particularly al-Qaeda, are notable. They have adopted strategies of global jihadist movements, as seen in their allegiance to al-Qaeda and coordinated propaganda efforts. This relationship is highlighted by parallel attacks and shared rhetoric with other extremist groups, suggesting a synchronised approach influenced by al-Qaeda's media strategy.

The use of digital tools in IO by various groups, including terrorists and governments, has become increasingly prevalent in recent years. In the context of Somalia, both the Shabab terrorist group and the Somali government have leveraged digital platforms for their respective information campaigns.

Shabab's SDIOs include the use of social media in which they must spread propaganda, recruit members, and disseminate information about their attacks. This includes the use of X (formerly Twitter), Meta (formerly Facebook), and other platforms to reach a wider audience. They also use online Forums and websites that they often use to disseminate their ideology,

communicate with sympathisers, and coordinate activities. They also engage in cyber warfare tactics, including hacking and cyberattacks against government or other targets. The Somali Government's Digital Efforts include Counter-Propaganda Campaigns, whereby the government employs digital platforms for counter-propaganda efforts to combat the narratives put forth by Shabab. Recently, they have also started public awareness and education campaigns utilising social media and digital tools informing the community about the risks and realities of terrorism.

For over a decade, the terrorist organisation Shabab, based in Somalia, has strategically emphasised media engagement as an essential facet of its propaganda and recruitment initiatives. Recently, the group has intensified its efforts on social media, leveraging influencers to disseminate its narratives and official communications, including press releases and videos. The specific functions these influencers fulfil within the operational hierarchy of Shabab remain inadequately understood. Consequently, this gap in understanding represents a significant oversight in the ongoing international efforts to counter Shabab (Anoba 2017).

The Shabab Social Media Influencers

This analytical insight discusses the pivotal role social media influencers play within Shabab, underscoring their critical contribution to the terrorist group's operations. These influencers transcend the role of mere "fanboys" – enthusiasts or sympathisers – and emerge as vital proponents in supporting the group's activities and recruitment processes. To elucidate the role of influencers in Shabab, this study scrutinises the May 2023 attack in Buulo Mareer, a case where Shabab claimed to have killed over 130 Ugandan soldiers. An analysis was conducted on the activities of Shabab influencers across platforms such as Facebook, Telegram, TikTok, and other lesser-known media, focusing on a three-week period surrounding the attack. This analysis contrasts their content and methodologies with the communications strategies of the counter-Shabab campaign. The findings highlight the significant impact influencers have in controlling the narrative online, which poses challenges to the efforts of the Somali government and the international community in their renewed endeavors to diminish the group's influence in the region.

On the day in question, the communication terrain was overwhelmingly influenced by Shabab, with social media influencers playing a pivotal role in the dissemination and generation of content. Notably, Telegram channels affiliated with Shabab were the first to report the incident, preceding even the group's web-based media outlets. This sequence of events suggests a direct line of communication between some influencers and Shabab's field operatives. One Telegram account, which was connected to influential Facebook

accounts, reported the event mere minutes after its commencement, implying foreknowledge of the attack.

In stark contrast to the Islamic State's communication strategies among its African affiliates, where official statements and photographic evidence of attacks are often delayed by days or weeks, Shabab's social media network exhibits a highly efficient and prompt operation. Influencers provided almost instantaneous updates during the attack, shared photographs on the same day, and orchestrated a unified narrative across a broad spectrum of influencers and platforms. In the immediate aftermath of the attack, these influencers directed followers to specific articles and radio programs, consistently echoing and amplifying messages from top influencers and centralised channels, thereby demonstrating the cohesive nature of the group's communicative framework.

The international community's response to this attack was markedly reactive. Shabab had already utilised its social media platforms to report on the conflict through its media outlets and released an official statement in both Somali and English before ATMIS publicly acknowledged the attack on Twitter. Furthermore, prior to ATMIS issuing their official press statement, Shabab's media agency, al-Kataib Foundation, had disseminated official photographs of deceased and captured Ugandan soldiers to an extensive audience across their networks. A notable instance was a TikTok post by a prominent influencer, which garnered over 300,000 views, featuring a photo of a captured Ugandan soldier.

However, this author's research found out that key area that the Somali government have overlooked is collaboration with the local tech companies and the introduction of robust cybersecurity measures, to protect government data and infrastructure from potential cyberattacks by terrorist groups. While the digital terrain provides both opportunities and challenges for IO in conflict zones like Somalia, the dynamic between terrorist groups and government entities in this realm is complex and continually evolving. They commonly use social media to disseminate their messages or propaganda. They may also engage in cyberattacks, but these are typically less sophisticated than those of state actors. Phishing campaigns, website defacements, and distributed denial-of-service (DDoS) attacks are common tactics (Anoba 2017). The Shabab terrorist group uses effectively the hash tagging to facilitate the establishment of ad hoc social interaction groupings or subcommunities, which constitute a temporal habitat for IO. The use of hash tagging itself is not new, as it has been employed and proven effective across platforms, from "influencers" and organisations to disinformation operations, for acquiring followers and increasing exposure (Niblock et al. 2022). This is a powerful tool that enables them to recruit followers and spread their ideology.

This author has noticed that most of the valid URLs in the Shahab profiles redirect to accounts on other social networking sites like Facebook,

Instagram, and YouTube and to blogs with little or no regulations. They also use domains registered in less regulated environments like those country code Top-Level Domain Names (ccTLD) within the Australian Jurisdiction and yet run private entities as in Norfolk Island and Christmas Island. This is beyond the scope of this chapter; however, it is worth mentioning as it highlights the challenges in this sector. For example, .au is not the only top-level domain name assigned to Australia. Some Australian territories have their own ISO 3166–1 alpha-2 code, and therefore have their own ccTLD as well:

- .cx – Christmas Island
- .cc – Cocos (Keeling) Islands
- .nf – Norfolk Island
- .hm – Heard and McDonald Islands

As the appropriate authorities were late in recognising the need to manage these, most were registered by entrepreneurs for use as vanity domains unrelated to the locale they serve. For example, .cc is now operated by VeriSign. hm represents a nature preserve with no human inhabitants.

Some Australian local government authorities have adopted *.cc domains as a convenient abbreviation for "City Council." For example, the Brisbane City Council uses the domain name "bne.cc" as a URL shortener. This is a loophole many non-state actors and terrorists take advantage of. What this highlights is that the challenges of managing and regulating IO require collaboration between government, UN agencies assigned to technology sectors such as the International Telecommunication Union (ITU), as well as NGOs involved in this sector such as Internet Corporation for Assigned Names and Numbers (ICANN), Internet Society, and others.

How to Deal With Digital Jihad?

The current strategy against Shabab focuses on military, financial, and ideological dimensions, yet it inadequately addresses the group's pervasive online influence and ground-level presence, elements crucial for long-term stability in Somalia. Shabab's online networks function as an additional battlefront. While traditional security measures may yield sporadic successes in reclaiming territories or disrupting financial networks, the struggle for ideological dominance persists, primarily through social media. Neglecting Shabab's dominance in these digital arenas may inadvertently bolster their recruitment capabilities and regional influence (Anoba 2017). The fight against this digital jihad transcends mere content regulation or systematic removal of social media content for several reasons: In response to content removal and

enhanced moderation on major platforms, Shabab is diversifying its online presence.

On mainstream platforms, Shabab affiliates display resilience against account suspensions. A prominent influencer, for example, was banned from Facebook six times in three weeks. Each time, they promptly created a new account, announced it on Telegram, and rapidly reconstructed their network. This pattern indicates not only resource availability but also a sophisticated understanding of circumventing platform security measures. Shabab's coordination across its digital networks outperforms the collective content moderation efforts of social media companies. Eliminating their content from one platform barely impacts their broader network. A comprehensive approach to mitigate Shabab's threat must include tackling their online activities. Recognising digital jihadists as integral to Shabab's resilience strategy is vital. This approach necessitates a multifaceted strategy that extends beyond conventional security measures, aiming to diminish the group's ground and online influence. Effective countermeasures should encompass understanding and disrupting the flow of information within social networks. In the context of an increasingly digital terrain, even in conflict-impacted states like Somalia, undermining a terrorist organisation's physical presence is insufficient without addressing its digital foothold.

Discussion and Conclusions

The chapter has covered distinctions between state and non-state actors in digital IO which is marked by differences in resources, objectives, and methodologies. While state actors demonstrate more sophistication and strategic depth, non-state actors are characterised by their adaptability and opportunistic nature. Understanding these differences is essential for developing effective strategies to counter malicious activities in the digital domain.

Samantha Bradshaw and Philip N. Howard (2018) from the University of Oxford captured the main issues in their paper "Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation" when they highlighted that the phenomenon of cyber troops, which are government, military, or political party teams, is committed to manipulating public opinion over social media. Their paper provides a comprehensive inventory of major organisations behind social media manipulation across 28 countries, detailing their messages, strategies, organisational forms, and capacities including budgets and staffing. It highlights the pervasive and global nature of cyber troops, the transition from military units to strategic communication firms for organising these troops, and the varied tactics employed, such as creating fake accounts, deploying bots, and engaging in content creation for political propaganda. The study also differentiates between the involvement

of authoritarian regimes and democracies in social media manipulation, noting that both target domestic and foreign publics but in diverse ways.

State actors engage in more coordinated and strategic IO with global reach and significant geopolitical impact, focusing on disinformation campaigns and targeting critical infrastructure. Non-state actors, while increasingly adopting cyber capabilities, typically have limited capacity unless acting as proxies for states. Their operations are marked by financial motivations, ransomware attacks, and a degree of unpredictability due to diverse motivations. The intersection of state and non-state actors in cyber operations presents a complex and dynamic terrain in digital information warfare.

A primary focus of state-led IO is the dissemination of disinformation, frequently linked to political campaigns and social media manipulation. Studies have offered global overviews of state-backed IO, revealing patterns of coordination across different geographical settings and historical periods. Nation-states like China, Russia, Iran, and North Korea have been identified as leading actors in cyber espionage, focusing on targeting critical infrastructure and conducting large-scale disruptive cyberattacks.

Non-state organisations, including patriotic hacking collectives and ransomware groups, have increasingly adopted offensive cyber capabilities to further their strategic objectives, making countermeasures more challenging. Powerful non-state armed groups often act on behalf of a state, as in performing proxy operations,[1] offering plausible deniability. This outsourcing reduces the barrier to entry into modern conflicts and allows states to pursue riskier strategies.

And finally, the following are actionable recommendations and countermeasures for governments, organisations, and individuals on how to safeguard against malicious digital campaigns. This will include, as an outlook, strategies for promoting the responsible use of digital tools in the information space and speculation on how evolving technology might change the way state and non-state actors engage in these operations and what this means for global security and policy formulation.

To diminish the media voice and grasp of non-state actors or terrorists such as the Shababs in Somali, it is recommended that the government should focus efforts on improving the usage of advanced IO tools and promulgate content on their web-based media and radio stations, adapting it to new target audiences and expanding their range to rural areas that have long been excluded from the government's outreach.

Note

1 https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace/#:~:text=Without%20proper%20legislation%2C%20states%20using,to%20governments%2C%20businesses%2C%20and%20individuals

References

Anoba, I. 2017. How foreign aid hurts famine relief in Somalia. *Foundation for Economic Education (FEE)*, March 28. https://fee.org/articles/how-foreign-aid-hurts-famine-relief-in-somalia

Benkler, Y., Faris, R. and Roberts, H. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.

Bradshaw, S. and Howard, P.N. 2018. The global organization of social media disinformation campaigns. *Journal of International Affairs*, 71(1.5), pp. 23–32.

Cadwalladr, C. and Graham-Harrison, E. 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*.

Center for Strategic and International Studies (CSIS). 2022. *Emerging Cyber Threats: No State is an Island in Cyberspace*. https://www.csis.org/analysis/emerging-cyber-threats-no-state-island-cyberspace [Accessed 4 Apr. 2024].

De Poli, B. 2017. *Marketing and Advertising Terrorist Propaganda: An Analysis of Modern Means and Methods used by Islamic Terrorist Organizations*. Ca' Foscari University of Venice.

The Economist. 2017. Sharp power: The new shape of Chinese influence. *The Economist*, December 14. https://www.economist.com/christmas-specials/2017/12/14/sharp-power-the-new-shape-of-chinese-influence

Hansen, S. 2013. *Shabab in Somalia: The History and Ideology of a Militant Islamist Group 2005–2012*. C. Hurst & Co.

Langner, R. 2011. *Stuxnet: Dissecting a Cyberwarfare Weapon*. IEEE Security & Privacy.

Niblock, I., Wallis, J. and Zhang, A. 2022. *Understanding global disinformation and information operations: Insights from ASPI's New Analytic Website*. Barton, Australian Capital Territory: Australian Strategic Policy Institute. http://nla.gov.au/nla.obj-3049417400 [Accessed 9 Sep. 2025].

Ordoñez de Pablos, P. 2023. Editorial: "Digital tools, innovation, and competitiveness: Lessons for the digital transition." *Journal of Science and Technology Policy Management*, 14(1), pp. 1–5.

Pearlman, L. 2019. *Tweeting to Win: Shabab's Strategic Use of Microblogging*. Yale Review of International Studies.

Perloff, R.M. 2021. *The Dynamics of Political Communication: Media and Politics in a Digital Age*. Routledge.

Postill, J. 2018. Populism and social media: A global perspective. *Media, Culture & Society*, 40(5), pp. 754–765.

Posetti, J. and Matthews, A. 2018. A short guide to the history of 'fake news' and disinformation. *International Center for Journalists*, 7, p. 2018–07.

Rajtmajer, S. and Susser, D. 2020, September. Automated influence and the challenge of cognitive security. In *Proceedings of the 7th Symposium on Hot Topics in the Science of Security* (pp. 1–9).

Starbird, K., Arif, A. and Wilson, T. 2019. Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), pp. 1–26.

Waltzman, R. 2017. *The Weaponization of Information: The Need for Cognitive Security*. RAND Corporation.

Wang, X., Li, J., Srivatsavaya, E., et al. 2023. Evidence of inter-state coordination amongst state-backed information operations. *Scientific Reports*, 13, 7716.

Yilmaz, I., Akbarzadeh, S. and Bashirov, G. 2023. *Comprehending Strategic Digital Information Operations (SDIOs)*. Populism & Politics (P&P), European Center for Populism Studies (ECPS).

14

ALT-RIGHT IDEOLOGY, MASCULINITY, AND THE STRATEGY OF INFORMATION OPERATIONS

Understanding Digital Dissonance

Aiden Aylett, Toija Cinque, and Jodi McAlister

Introduction

The integration of Application Programming Interfaces (APIs) across social networks has transformed community shaping and engagement, enabling seamless content dissemination and personalised user experiences (Nawaz et al. 2023). Recommendation algorithms leverage data access to curate content feeds tailored to individual user interests and behaviors (Peukert et al. 2023). This can contribute to the formation of "filter bubbles," potentially isolating users within echo chambers. This chapter critically examines the role of digital platforms in strategic information dissemination by looking at podcasts by Alex Jones, Andrew Tate, and Ben Shapiro, which cater to – and isolate – audiences ranging from traditionally conservative to far-right.

We analyze their actions within the framework of SDIOs (Yilmaz et al. 2023). SDIO narratives are crafted to resonate with intended audiences, utilising psychology, culture, and emotions to draw listeners into self-reinforcing cycles of confirmation bias and manipulation (Yilmaz et al. 2023, 3). These podcasts each use a combination of medium and language to create narratives aligning with the pre-existing ideological foundations of listeners. We analyze episodes of each podcast using Steven Hassan's BITE model and Influence Continuum, employ Voyant to discuss common or repeated phrasing, and discuss the feelings of intimacy between speaker and listener audio can engender (Rodero & Lucas 2021). Yilmaz et al. (2023) argue that SDIOs "aren't always coordinated by automated bots or pre-planned campaigns" but can "happen naturally through implicit coordination among various participants" (3). They are thus " 'cooperative' endeavours in that they do not always rely on mere 'bots' and 'trolls,' but also encompass the contribution

DOI: 10.4324/9781003628088-19
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

of online crowds (both knowingly and unknowingly) in the propagation of false information and political propaganda" (Yilmaz et al. 2023, 3). The overlapping audience of these podcasts, and the disinformation and political division they sow, could be characterised as a "conspiratorial public" (Fitzgerald et al., Chapter 4): "networks of individuals who collectively work to promote and sustain conspiratorial narratives on social media."

While these podcast hosts may not actively engage in deliberate strategic information manipulation, their encouragement of conspiratorial thinking contributes to the spread of misinformation and disinformation. This has fostered implicit coordination among their communities, leading to significant social impacts like the harassment of victims' families following Jones's denial of the Sandy Hook shooting (Hyzen & Van den Bulk 2021), Tate's contribution to misogyny in Australian schools (Wescott et al. 2023), and Shapiro's role in spreading media distrust and reframed far-right rhetoric (Dowling et al. 2022; Speakman & Funk 2020). These hosts frequently advocate for traditional masculine roles while challenging political correctness, aligning themselves with far-right ideologies (Sunderland 2023).

Like alt-right groups, these hosts exploit digital platforms, especially social media, to propagate their ideologies, manipulate public sentiment, and control followers' perceptions (Salojärvi et al. 2023). This reflects broader online narrative strategic trends, with figures presenting themselves as arbiters of "authentic" masculinity and gatekeepers to an idealised lifestyle, often complemented by online courses, health supplement promotions, and wealth-creating (Woolley & Luger 2023). We posit that the hosts' digital engagement exemplifies authoritarian control, manifesting in the dissemination of misinformation and reframed far-right rhetoric. This, coupled with elements of authoritarian control, significantly influences individuals vulnerable to political radicalisation (Grossman 2017). The alt-right aims to captivate vulnerable young people, capitalising on their search for identity (Acheson & Papadima 2023; Subrahmanyam & Šmahel 2011). We stress the importance of critical digital media literacy in countering such strategies.

This chapter explores communication strategies used in *The Alex Jones Show*, *Tate Speech*, and *The Ben Shapiro Show*, analyzing linguistic features, emotional appeals, and audio techniques for potential impact on audience perception and susceptibility to persuasion. These strategies include emotive and cryptic language, appeals to scientific authority, and potent political oratory. We also consider the audio context. Audio media can engender the "human emotional intimacy effect" (Rodero & Lucas 2021): listening to another person tell you a story is very powerful – particularly when headphones collapse the barrier between "the contained and container" (Stankievech 2007, 59), allowing sound to cocoon the listener in a kind of "hyper-intimacy" (Spinelli & Dann 2019, 84; see also Bellas & McAlister 2023; Bull & Back 2003; Madsen & Potts 2010) that may add another layer to podcasts' persuasive

abilities (Pettman 2017, 4). The visual aspects of these podcasts, in which presentational choices play a crucial role, are out of scope in this chapter, but this would be fruitful ground for further research. While we focus on podcasting, it is crucial to acknowledge how social media platforms facilitate the dissemination of condensed video materials, such as clips and sound bites, thus extending the reach of these podcasts beyond their native environments (see Robson 2023). Broadly, this chapter endeavors to illustrate the sophisticated use of digital media in non-state information campaigns which normalise the ideological foundations of more radical right-wing communities and contribute to the broader acceptance of conspiratorial rhetorics.

The Alt-Right's Online Influence Operations

In digital IO terrains, podcasts can act as gateways for young men into the alt-right, a movement encapsulating a range of ideologies and strategies that interact with broader sociopolitical terrains. This section outlines discussions surrounding this movement and its use of digital platforms for spreading its ideology, especially within an SDIO framework.

The Alt-Right

Alt-right ideologies are underpinned by a distinct form of masculinity intertwined with politico-cultural conservatism. Nagle partially attributes the alt-right's rise to reactions against perceived progressive excesses, including feminism and multiculturalism. Main (2018) identifies rejection of liberal democracy as a core ideological principle, marked by a denial of the idea that all individuals are inherently equal (8). He also notes their "white racialism" (Main 2018, 8), a belief system prioritising the interests of white people, thereby advocating for their political dominance.

"Alt-right" encompasses a spectrum of beliefs and extremism: it is not a monolith. The "alt-lite," for instance, is skeptical toward mainstream political narratives and cultural diversity but stops short of endorsing a white ethnostate. This delineation is further elaborated in the works of scholars like Neiwert (2017).

"Masculine" Identity

The alt-right co-opts narratives of traditional masculinity, positioning itself as a defender of an endangered male hegemony (Menzie 2022). This is critical to its appeal and cohesion, providing a sense of identity and community, framing political adversaries as threats to traditional gender roles, and mobilising followers through a perceived need to defend them. As it evolved, it incorporated elements from the "manosphere," an intersecting misogynistic

online subculture similarly positioning masculinity as under attack (Hermansson et al. 2020, 163). These online spaces serve as breeding grounds for radicalisation, where disaffected men are indoctrinated into a worldview intertwining misogyny with far-right ideologies (Ging 2019). This amalgamation forms a core component of the alt-right's identity and modus operandi.

Digital Dissemination

Marwick and Lewis (2017) examine how the alt-right exploits digital ecosystems to disseminate messages, recruit followers, and create insular communities, underscoring the transformation of online spaces into echo chambers where extremist ideologies proliferate. These activities align with SDIOs' objectives and methods, using digital tools to influence public opinion, manipulate political processes, and sow discord (Starbird et al. 2019): something further compounded by platform algorithms, which often prioritise content that generates engagement, regardless of ideological leanings. The ability to shift public discourse toward extremist positions, and social media's capacity to spread extremist ideology, presents a unique challenge to democratic societies (Lyons 2017). The alt-right exploits these vulnerabilities to exert influence far beyond their immediate sphere. They implement a distinct communication strategy marked by irony and meme-culture to spread ideologies in ways often opaque to outsiders but which resonate deeply within in-groups, serving as a gatekeeping mechanism that demarcates the boundaries of their community (Phillips & Milner 2017). Their digital platform use is a multifaceted phenomenon, intertwining political, racial, and gender ideologies with various cult-like tactics. Understanding this is crucial for comprehending the movement's influence and impact.

Cult Tactics and SDIOs

The alt-right's ultimate objective is to disrupt established political narratives, thereby remaking the sociopolitical terrain in alignment with its vision of hegemony. This objective is an SDIO objective, of the kind which "happen naturally through implicit coordination among various participants" (Yilmaz et al. 2023, 3). Aspects of alt-right digital IO contain tactics seen in models of authoritarian cult control. Hassan (2020) discusses how cults exert influence over their members for the purposes of control, a trait also observable in the alt-right's IO. While critics argue Hassan's work "lacks scientific rigor and empirical evidence," it provides a good observational framework for discussing influence and control in groups considered destructive or unhealthy – Hassan himself is an ex-member of a high-control group (Teply 2023, 11). The BITE model of authoritarian control (see Hassan 2020, 52–56) includes four ways a group might control its members: behavior, information, thought, and

emotional control. The model highlights behavior and information control (Hassan 2020, 52–54) as key tactics used by authoritarian groups and digital influencers. Behavior control regulates individuals' actions, associations, and beliefs through isolation, rigid rules, and social pressure, while information control manipulates access to knowledge by distorting facts, discrediting outside sources, and restricting critical perspectives. Figures like Jones, Tate, and Shapiro employ these to shape public perception, create ideological echo chambers, and foster parasocial loyalty. This underscores how such tactics drive online radicalisation, emphasising the need for critical digital media literacy to counter it.

Additional aspects of the BITE model of authoritarian control illustrate how thought and emotional control are used in coercive groups (Hassan 2020, 54–56). Thought control enforces ideological conformity through binary thinking, identity shifts, loaded language, and memory manipulation, suppressing critical thought via denial and rationalisation. Emotional control fosters guilt, fear, and dependence, making members feel inadequate while instilling fear of leaving, reinforced through public shaming and demonisation of ex-members. These tactics, evident in alt-right podcasts, shape perceptions, suppress dissent, and normalise extremist views by leveraging digital platforms for ideological conditioning and emotional manipulation, reinforcing radicalisation through persuasive rhetoric. Hassan recommends that this model be paired with the Influence Continuum (see Hassan 2020, 50), a model positing cult groups use BITE model tactics to influence people into destructive and unhealthy behaviors and relationships. Hassan's Influence Continuum (2020) presents a conceptual spectrum ranging from constructive, healthy forms of influence to destructive, unhealthy control. It categorises influence at three levels – individuals, leaders, and organisations – highlighting distinct attributes on either side. On the constructive end, individuals retain authenticity, critical thinking, and experience unconditional positive regard. Leaders are characterised by psychological health, accountability, and empowerment of others. Organisations foster egalitarianism, informed consent, and personal growth. Conversely, the destructive side features identity manipulation, coercive dependency, and emotional control in individuals; narcissism, secrecy, and authoritarianism in leaders; and manipulative, elitist, power-preserving structures in organisations. The model underscores how influence can range from benign to coercive, providing a framework for analyzing power dynamics across personal, social, and institutional contexts.

In sum, the Influence Continuum (Hassan 2020) illustrates the continuum between constructive and destructive influence such that healthy influence fosters critical thinking, authenticity, and empowerment. Unhealthy influence enforces dependency, fear, and authoritarian control. For individuals,

this contrast is seen in the promotion of free will versus ideological conformity; for leaders, it distinguishes trustworthy authority from narcissistic, power-hungry control; for organisations, it contrasts egalitarianism with manipulative elitism. This framework mirrors how alt-right digital figures create ideological echo chambers, fostering dependence while suppressing dissent. Presenting influence as a spectrum rather than a binary underscores the importance of critical media literacy in recognising and resisting manipulative digital strategies. We use the BITE model and Influence Continuum together to analyze how these podcasts employ misinformation, disinformation, and indoctrination – alongside the tactics of destructive groups – to attract and retain audiences.

A Methodological Framework for Analyzing Alt-Right Masculinity in Podcasts

This chapter examines how key podcasts function as gateways for the alt-right by targeting young men who feel disenfranchised. We use a mixed methods approach to explore how these digital platforms are used for strategic information dissemination and audience engagement. The primary podcast audiences are likely individuals sympathetic to alt-right ideologies, particularly those related to "traditional" masculinity. They might be seeking affirmation or simply be curious or vulnerable to such narratives. We ask two questions:

RQ1: To what extent do these podcasts use authoritarian rhetoric, and what effect might this have on listeners?
RQ2: What role does authoritarian masculinity play in these podcasts?

Method

We analyzed *The Alex Jones Show*, *The Ben Shapiro Show*, and *Tate Speech*, three popular right-wing podcasts. Jones blends conspiracy theories with ideological narratives, using emotive language and masculinity to position LGBTQ individuals, feminists, and identity politics as threats to traditional values (Hyzen & Van den Bulke 2021). He exploits social media, particularly X/Twitter, to amplify political divisions (Ross & Bhatia 2019). Tate spreads alt-right conspiracy theories on vaccines, masks, and gender roles (Miller 2023), targeting young men across platforms, including Rumble, where his content is widely shared (Wescott et al. 2023). Shapiro, while rejecting white nationalism and conspiracy rhetoric, employs similar ideological frameworks, particularly on immigration and media distrust, aligning him with alt-lite narratives (Speakman & Funk 2020).

Episode Selection

We examined episodes explicitly discussing masculinity:

- *Tate Speech*: *Tate on Being the Best* or *TOBTB* (13-07-2022, 5:56), *Tate on Hollywood and Masculinity* or *TOHM* (08-07-2022, 10:52), and *Tate on Men Paying for Dates* or *TOMPD* (08-07-2022, 5:11).
- *The Ben Shapiro Show*: *Why Are Men in Crisis* (19-07-2023, 1:03:28).
- *The Alex Jones Show* (25-10-2022, 3:59:56).

We selected three shorter *Tate Speech* episodes to balance the longer Jones and Shapiro episodes. The SoundCloud version of Shapiro's episode was used due to its slightly longer runtime.

Results and Findings

We employed Voyant Tools, a suite of digital tools designed by digital humanists Stéfan Sinclair and Geoffrey Rockwell, to visualise and analyze language use in transcripts of each podcast episode. We assessed these episodes through the BITE model, identifying language usage and rhetorical frameworks which fit one of the four elements – behavior, information, thought, or emotional control – alongside the Influence Continuum model, to help determine authoritarian control. This analysis is purely illustrative, based on the presented content, and not an assertion that texts or authors are engaged in cult-like practices; however, cult-like rhetoric is certainly observable.

The Alex Jones Show

This covered a wide range of topics, including politics, conspiracy theories, and product promotion, all framed in a highly charged, biased narrative. Figure 14.1 showcases the frequency of words used. "People" is among the most prominent, suggesting discussion about people or opinions. The words "info" and "infowarsstore.com" likely refer to the websites that host the podcast and advertise various products. Words like "globalist," "world," "fight," "think," "new," "today," and "support" underscore the themes critically evaluated later involving current events, opinions, and political/ideological discussion by the host.

This visualisation in Figure 14.1 underscores persuasive and emotionally charged language, aligning with SDIOs and the BITE model. The most prominent words – "know," "that's," "it's," "people," and "going" – reflect conversational and declarative speech patterns, reinforcing certainty and authority. Jones frequently uses "know," signaling assertion of truth or insider knowledge, a tactic often seen in conspiracy rhetoric. Similarly, "people"

FIGURE 14.1 *The Alex Jones Show* Word Cloud.

and "they're" indicate collective identity formation, reinforcing in-group/out-group dynamics (a central feature of alt-right discourse). Key terms like "fight," "war," and "globalist" suggest an adversarial worldview, emphasising conflict and struggle. This aligns with Hassan's emotional control category, as fear-driven narratives are used to galvanise audiences into action. Additionally, commercial elements such as "infowarstore.com" and "products" highlight how monetisation is intertwined with ideological messaging, supporting research on the financial incentives behind alt-right digital influencers. This word cloud provides empirical evidence of repetitive linguistic framing, shaping audience perceptions and reinforcing conspiratorial thinking. The conversational structure, frequent personal pronouns ("I'm," "we're," "you're"), and high emotional intensity contribute to parasocial bonding, enhancing audio's persuasive power. This offers insight into how digital figures like Jones strategically construct narratives to influence and mobilise their audiences.

Behavior Control

Podcast listeners are urged to engage in political activism and purchase specific products (e.g., vitamin supplements) to both support the cause and address a manufactured health crisis. Anxiety is instilled through fear-based messaging, claiming that these products are essential for survival ("without

these things you die" 5:31) and warning of environmental dangers ("so much of the food is debased" 5:34). These claims ("helps every cellular function of the body" 5:22) lack scientific backing, yet are reinforced through repeated calls to action ("it funds the info war . . . the only way you lose is not taking action today" 5:48), with the product advertised 11 times.

This consumption-driven behavior control extends to political direction. Jones dictates how listeners should interpret global events without citing specific sources ("30-plus prominent Democrats . . . send a letter to the puppet Joe Biden"), reinforcing distrust in mainstream politics. He positions public opinion as overwhelmingly aligned with his views ("99 percent of humanity . . . does not want thermonuclear war" 1:31), blending behavior and information control to shape audience beliefs and actions.

Information Control

Jones selectively presents misinformation and conspiracy theories to frame political opposition negatively and distort geopolitical issues. He suggests that the Ukraine war is a "false flag" (2:41–2:57), claiming that when "the globalist deep state" feels threatened, it will stage a false flag attack (3:42–4:07). He promotes the "elite capture" conspiracy (20:29), alleging that the Chinese Communist Party (CCP) has infiltrated US politics, culture, and economy (21:24–22:30). His vague reference to "individuals running Hollywood" (21:34) is an antisemitic dog whistle, reinforcing the Jews-control-Hollywood trope (Hern 2015). He positions these groups as part of a globalist agenda, linking them to the WEF, private banks, and the EU, while praising Alberta Premier Danielle Smith for opposing vaccines and the New World Order (6:32–7:21). Jones' information control relies on selective reporting, fearmongering, and discrediting mainstream media, positioning him as the only reliable source of truth. By presenting theories as facts without evidence, he manipulates perceptions, fostering distrust in traditional institutions while reinforcing his ideological narratives.

Thought Control

Framing narratives in terms of us versus them or good versus evil – "amazing" leaders (1:50:24) versus the Biden "puppet" (0:52, 7:49) – promotes a limited worldview, discouraging complex understanding or critical thinking while promoting conspiratorial thinking. Moreover, predicting dire consequences without substantial evidence can influence thought patterns, making individuals more susceptible to fear-based decision-making. Jones frequently alludes to catastrophic outcomes if his advice is not followed or if the audience does not align with his views: for instance, suggesting that failure to act against the "globalist" agenda will lead to societal collapse or war. He

appeals to notions of good sense, telling his audience "Seems like pretty common sense to me" (1:29) and "I believe them" (4:00).

Emotional Control

Jones exploits fear of societal collapse, war, and loss of freedoms to maintain audience anxiety and panic, a key aspect of emotional control. Guest Hotep Jesus frames public backlash against a Korean-American artist's anti-Black Lives Matter comments as evidence of domination of Asians by "the other," reinforcing racial division and victimhood ("they like us as their little pets" 3:07:56–3:08:13).

Jones further cultivates paranoia and mistrust, portraying critics and political opponents as existential threats. He brands himself the "number one enemy" of globalists, asserting that their obsession with silencing him proves his truth-telling. He reframes sharing his content or purchasing his products as an act of resistance, positioning his audience as the "tip of the spear" (28:59–29:54). This us-versus-them rhetoric fosters emotional dependency, where listeners see Jones as a protector and the outside world as a threat, ensuring loyalty and reinforcing ideological isolation.

Influence Continuum Model Application

The Influence Continuum model assesses how influence tactics are applied. Jones' use of fear, misinformation, and polarising language could be indicative of attempts at undue influence, moving toward the more authoritarian end of the continuum. The explicit promotion of products and political ideologies under the guise of resistance further suggests efforts to manipulate readers' perceptions and actions for specific ends. The conspiratorial tone indicates the prioritisation of an us-versus-them mentality, which can lead to distrust of outside sources.

Tate Speech

Figure 14.2, generated from Andrew Tate's "Tate on Being the Best" (*TOBTB*), highlights dominant linguistic patterns, emphasising self-referential speech ("I'm," "you're") that fosters audience engagement and parasocial intimacy. Aggressive, hyper-masculine terms ("fucking," "bitch," "guy," "man") align with Tate's manospheric ideology, reinforcing dominance and competitiveness. The prominence of "James Bond" reflects aspirational masculinity, while words like "war" and "world" suggest an us-versus-them mindset, fostering thought and emotional control. Urgent phrasing ("need," "important") reinforces dependency on his guidance, while references to "drug" and "dealers" support moral superiority narratives. Overall, this shows how

FIGURE 14.2 *Tate on Being the Best* Word Cloud.

Tate's rhetoric promotes hierarchy, struggle, and ideological conformity, tactics often used in alt-right and manosphere recruitment strategies.

Figure 14.3, generated from Andrew Tate's "Tate on Hollywood & Masculinity" (*TOHM*), highlights themes of masculinity, power, race, and aggression. The prominence of "Bond," "James," and "money" reinforces Tate's idealised vision of dominance and wealth, while frequent explicit and violent language ("fucking," "attack," "gun," "kill") reflects his confrontational, hyper-masculine rhetoric. Racial terms ("Black," "White," "racist") alongside words like "female," "she's," and "character" suggest discussions of gender roles and identity politics, likely framed against progressive narratives. The term "Penny" can refer to Moneypenny, indicating a critique of Hollywood's portrayal of gender. This "us-versus-them" framing, seen in words like "attack," "liberals," and "warroom," aligns with emotional and thought control tactics, fostering paranoia and resistance to cultural change. Overall, Tate's rhetoric promotes traditional masculinity, hierarchy, and distrust of progressive media.

Figure 14.4, generated from Andrew Tate's "Tate on Men Paying for Dates" (*TOMPD*), highlights themes of gender roles, money, and value, reinforcing hyper-masculine, transactional views of relationships. The prominence of "pay," "women," "value," and "high" suggests focus on financial expectations in dating, aligning with notions that a man's worth is tied to wealth and dominance. Frequent use of explicit language ("fucking," "bullshit") and derogatory terms ("bitch") reflects aggressive, demeaning discourse toward women. The contrast between "high" and "low" value

FIGURE 14.3 *Tate on Hollywood & Masculinity* Word Cloud.

FIGURE 14.4 *Tate on Men Paying for Dates* Word Cloud.

implies a hierarchical ranking of women, a common theme in misogynistic narratives. This framing aligns with emotional and thought Control tactics, as Tate reinforces rigid gender roles, financial dominance, and male entitlement, shaping audience perceptions of relationships through monetary and status-based metrics.

Overall, Tate's digital rhetoric employs authoritarian influence tactics, reinforcing rigid gender roles, ideological conformity, and emotional

dependency. His discourse dictates behavior, controls information, enforces binary thinking, and manipulates emotions to maintain audience loyalty and shape perceptions. Analyzing these patterns reveals how his messaging functions as a strategic mechanism of control, fostering an us-versus-them mentality and distrust of external perspectives.

Behavior Control

Tate frames obedience as a path to elite status, instructing followers to complete tasks without question ("You're going to Warsaw . . . I'm not gonna tell you what you're doing, but you're doing X, Y, Z." 3:46–3:55, *TOBTB*). His self-improvement courses promote financial success and control over women, implying a lesser life without them. He asserts men must pay for dates or risk being "low value" (1:11) and "not manly" (3:34), enforcing rigid gender roles and pressuring compliance (*TOMPD*).

Information Control

Tate positions himself as the sole reliable authority, dismissing outside information as manipulative ("The Last Hope" 4:08, *TOBTB*). He claims that masculinity is under attack by liberals and that only weak, controllable men are favored (2:56–3:12, *TOHM*). He refers to himself as "Big Daddy Tate" (0:18, 3:14, TOMPD), degrading dissenters as "morons," reinforcing us-versus-them rhetoric.

Thought Control

Tate urges followers to adopt his "warrior mentality" ("Cuz there's none fucking left." 4:41–4:46, *TOBTB*). He frames James Bond's Black female casting as an "attack on white people" (2:03) and "alpha males" (2:43), insisting whiteness and masculinity are under siege (*TOHM*). He enforces binary thinking – men are either dominant "alphas" (1:32) or "beta losers" (0:30), creating pressure to conform (*TOMPD*).

Emotional Control

Tate fosters guilt and unworthiness, claiming those who reject his ideology lack respect and status ("No one's ever been on my level." 4:50, *TOBTB*). He shames men as "bitch ass pussy ass" (3:37, *TOMPD*) for not paying for dates and devalues women who do not meet his standards as "ugly" (2:00, *TOMPD*). He instills fear, insisting that masculinity is under threat, using anger and outrage to strengthen audience loyalty (*TOHM*).

Influence Continuum Model Application

Tate's derogatory language, self-aggrandising statements, and binary worldviews place his tactics on the destructive end of the Influence Continuum. His messaging promotes binary thinking, distrust in external sources, and ideological isolation, reinforcing elements of authoritarian influence.

The Ben Shapiro Show

This episode of *The Ben Shapiro Show* discusses a range of topics, from men "falling behind by every single metric" to polarisation in politics, abortion, euthanasia, and American social policies. Figure 14.5, generated from the episode *Why Are Men in Crisis*, highlights key themes of gender roles, society, and morality, reflecting Shapiro's conservative ideological framing. The prominence of "men," "man," and "women" suggests a strong focus on gender dynamics, with discussions on masculinity, aggression, and societal expectations. Words like "society," "institutions," and "capitalism" indicate a broader critique of modern cultural and economic structures, reinforcing Shapiro's argument that traditional values are under threat (and women are at fault). Terms such as "toxic," "problem," and "aggressive" suggest debates around masculinity's perceived decline, while "right," "good," and "moral" reflect value-laden discourses distinguishing correct versus flawed

FIGURE 14.5 *The Ben Shapiro Show* Word Cloud.

social behaviors. The presence of "Andrew" implies references to Andrew Tate, linking the discussion to broader manosphere narratives. The word cloud illustrates how Shapiro frames gender relations as a societal crisis, positioning traditional masculinity as embattled while critiquing liberal and progressive perspectives on gender and morality.

Behavior Control

Shapiro frames moral issues such as abortion, euthanasia, and same-sex relationships in a way that aligns with conservative disapproval, while maintaining a veil of neutrality.

Information Control

Shapiro selectively distorts facts and frames opposing viewpoints as dishonest or unethical. For instance, he misrepresents book bans by suggesting they only restrict sexually explicit LGBTQ+ content, while dismissing Barack Obama's concerns as "absolute falsehoods" (56:58). He positions mainstream media as either "bamboozled" or negligent (11:05), reinforcing the idea that he and his audience hold exclusive access to truth.

Thought Control

Shapiro blends religious and scientific rhetoric to justify rigid gender norms. His arguments rely on binary thinking and straw-man fallacies, such as equating military-funded medical care for transgender individuals with "your taxpayer dollar is gonna pay for a man to cut off his penis" (40:08). He attributes toxic masculinity to changing female gender roles, asserting that the erosion of traditional femininity inevitably leads to male aggression (42:15). He further suggests men's economic and social struggles stem from problems with women at large (2:07–2:11), emphasising that men and women are biologically or divinely complementary (1:57–2:07). He also links economic decline to the breakdown of the traditional family, arguing that capitalism depends on men providing for wives and children.

Emotional Control

While less overtly combative than Jones or Tate, Shapiro operates through moralisation and fearmongering. He presents abortion as "killing your baby" (40:37) and euthanasia as making "the old . . . dispensable" (52:42), reinforcing guilt, shame, and fear. This creates an "us-versus-them" mentality, where progressive social changes are framed as existential threats to masculinity and Western stability.

Influence Continuum Model Application

Shapiro avoids direct calls to ideological warfare but still primes his audience for radicalisation through emotive language, moral absolutism, and the framing of alternative views as irrational. His approach cultivates distrust in mainstream discourse while positioning himself as a rational authority, subtly reinforcing patterns of ideological control and polarisation.

Discussion

As audio media, podcasts inherently cultivate intimacy and authenticity: crucial factors in the effectiveness of ideological messaging and audience persuasion. This intimacy is not merely a by-product of the format but is embedded in the nature of audio storytelling. The "human emotional intimacy effect" suggests that hearing a human voice fosters a sense of closeness and trust, triggering measurable emotional responses (Rodero & Lucas 2021, 14). This phenomenon is well documented in research on parasocial relationships (Tulley 2011; Bellas & McAlister 2023) and helps explain why figures like Jones, Tate, and Shapiro effectively establish deep psychological connections with their listeners.

A central paradox of podcasts is that they offer both personal space and communal experience. Listeners often consume them in private environments via earphones, reinforcing a one-on-one interaction with the speaker (Euritt & Korfmacher 2022, 192). This illusion of direct engagement makes rhetorical strategies more persuasive, as speakers frame their messages as confidential, urgent, and exclusive. Jones' conspiratorial narratives, Tate's hyper-masculine self-improvement rhetoric, and Shapiro's moral absolutism all thrive within this intimate auditory environment, where the speaker's voice is not just heard but internalised. The conversational tone and informal speech further enhance this effect, fostering parasocial bonds that cultivate loyalty and ideological alignment (Piper 2015; Korfmacher 2020).

This intimacy heightens the efficacy of behavior, information, thought, and emotional control tactics. Figures like Jones and Tate employ direct address, empowering listeners by positioning them as active participants in larger ideological struggles. This "us-versus-them" binary framing, a tactic central to authoritarian influence models, is amplified by the perceived personal connection between speaker and listener. Personal anecdotes, humor, and emotionally charged storytelling further reinforce this dynamic, fostering trust and ideological alignment over repeated exposure. Moreover, the podcast format allows speakers to build long-form narratives that are progressively radicalising, reinforcing ideological perspectives incrementally over time. This is particularly relevant in disinformation campaigns, where repetition and emotional reinforcement shape perceptions, encouraging loyalty to alternative

media sources while fostering distrust in institutions. Figures like these three hosts frame their messages as rational and evidence-based, despite deploying moralised rhetoric and binary thinking. By simultaneously positioning themselves as authorities and relatable figures, they maximise influence through an intimate, seemingly unscripted discourse.

Understanding the role of intimacy in audio media is, therefore, crucial to assessing how podcasts function as vehicles of ideological persuasion. As podcasts continue to shape public discourse, research on their affective and cognitive impacts remains imperative. Scholars such as Llinares et al. (2018) have highlighted the dynamic nature of digital communication and human connection, demonstrating that the illusory intimacy of the podcast medium is not merely an aesthetic feature but a core mechanism in the dissemination of ideological narratives.

Conclusion

In this chapter, we have examined *The Alex Jones Show*, *Tate Speech*, and *The Ben Shapiro Show*, three podcasts with varying degrees of proximity to the alt-right ideology. Rather than being explicitly alt-right, these podcasts operate as conduits that normalise and desensitise their predominantly young male audiences to alt-right ideas, potentially serving as gateways to further radicalisation. Our analysis reveals a spectrum of alt-right ideological usage, as well as a range of tactics from the BITE model employed to exert undue influence on listeners. They each promote conspiratorial thinking and distrust of alternate sources of information; as well as black-and-white thinking regarding issues of race, gender, sexuality, and political ideology. The episodes analyzed within *The Alex Jones Show* and *Tate Speech* were weighted heavily toward the authoritarian/destructive side of the Influence Continuum, while *The Ben Shapiro Show* episode framed similar ideological concepts in a less authoritarian manner.

Jones leverages his (and others') celebrity status in his show, blurring lines between his persona and personal identity to assume the role of a charismatic leader, guiding listeners towards what he portrays as the correct worldview (Hyzen & Van der Bulke 2021). In hypnotic and rambling monologues punctuated by news-like audio effects and a barrage of ads, Jones spreads alt-right ideology and fear via disinformation and conspiratorial frameworks, positioning Western society as under attack. He (and his guest hosts) target men who feel victimised by the feminism and #metoo movements, positioning those who disagree with them as satanists.

Tate utilises emotive language to target men who feel victimised by these movements, intertwining elements of the manosphere with alt-right ideology to promote authoritarian masculinity. He advocates for self-sufficient masculinity dependent on the domination of women. This contributes to a culture

of misogyny and male dominance, fostering an environment conducive to the acceptance of alt-right ideologies (Fleet 2022).

Through rapid-fire speech and intellectual language, Shapiro positions himself as an authority figure, while delegitimising traditional journalism, mainstream media, and places of higher education (Dowling et al. 2022). He disseminates recontextualised versions of alt-right ideology on topics such as immigration and the superiority of Western culture (Speakman & Funk 2020), although he does not overtly embrace the more actively and visibly racist discussions of white supremacist ideas like "the great replacement theory." Shapiro uses disinformation to frame divorce (5:03–5:39), abortion rights (41:36–46:18), and transgender rights (41:46–42:52) as a threat to Western culture.

These podcasts use the charisma of their hosts to spread misinformation, disinformation, and distrust toward alternative or mainstream sources. The five episodes analyzed each contrast so-called "acceptable" masculinities against unacceptable and dangerous masculinities. We observed the utilisation of parasocial intimacy to foster deep connections and trust between hosts and listeners, a technique that smaller political influencers use to generate "genuine engagement" (Woolley 2022, 121). Coupled with delivery styles and language choices, this creates an almost hypnotic effect which ritualises the listening experience in the lives of repeat listeners. This likely plays a role in the radicalisation of the target demographic: young men. The growing parasocial intimacy and trust in the hosts normalises the underlying ideologies, paving the way for more extreme viewpoints to appear reasonable.

We emphasise that while our study does not classify the alt-right as a cult nor label these podcast hosts as cult leaders, the application of the BITE model and Influence Continuum, highlights concerning authoritarian control and influence tactics in their content. These hosts act as non-state-funded political influencers, consistently using black-and-white rhetoric, conspiratorial frameworks, misinformation, and disinformation to influence their audiences, who then spread their talking points (operating as a "conspiratorial public," as defined by Fitzgerald et al. in Chapter 4). The lack of a specific leader in this disorganised and unstructured SDIO underscores the need for awareness and scrutiny of influential figures using similar tactics.

Future research into the correlation between tactics employed by destructive groups and non-state actors in SDIOs is recommended, along with investigations into the effects of podcasting and audio intimacy on radicalisation processes. Legislation and regulation of podcast platforms to mitigate harmful content must be approached with caution to differentiate between shows like *The Ben Shapiro Show* and more explicitly harmful podcasts, while media literacy teachings might benefit those susceptible to the rhetorical manipulation figures like Shapiro use to foster political distrust and division. Enhancing digital literacy and understanding of historical influence and

control in media and high-control groups is crucial in fostering an audience capable of discerning political discourse from fearmongering misinformation. By addressing these issues, we may mitigate the spread of radical ideologies online and safeguard against the potential harm they entail.

Index terms

Countries/Regions

- United States
- Australia
- United Kingdom (referenced culturally via Bond)
- Canada (reference to Alberta Premier)
- Russia (tangentially through discussion of alt-right parallels)
- China (in context of CCP elite capture conspiracy)

Institutions/Organisations

- Infowars/Infowarsstore
- *The Alex Jones Show*
- *Tate Speech*
- *The Ben Shapiro Show*
- Rumble
- SoundCloud
- World Economic Forum (WEF)
- Chinese Communist Party (CCP)
- Mainstream Media/Traditional Journalism
- Higher Education (as a domain of attack by alt-right influencers)
- US Government (referenced in conspiratorial framing)
- European Union (in conspiracy references)

SDIO Tactics

- Authoritarian masculinity reinforcement
- Parasocial bonding through audio intimacy
- Hyper-masculine branding via aggressive language
- Moral absolutism and value-laden framing
- Emotional manipulation through fear, shame, outrage
- Product monetisation interwoven with ideology
- Us-versus-them framing (in-group/out-group binary)
- Conspiratorial storytelling and "insider knowledge" claims
- Demonisation of critics and ideological opponents

- Repetition of loaded terminology and slogans
- Weaponised nostalgia (e.g., James Bond masculinity)
- Disinformation disguised as rationality or "common sense"
- Binary identity politics (e.g., "alpha vs. beta" males)
- False dilemmas and selective framing
- Anti-feminist and anti-progressive narratives
- Reductive critique of cultural shifts (e.g., casting in films)
- Use of economic and social anxiety as radicalising leverage
- Authority-building via intellectual tone or celebrity branding
- Implicit calls to action ("you must," "we must," "the last hope")
- Use of algorithms and cross-platform content repurposing
- Emotional intensity via rapid, hypnotic delivery
- Leveraging conspiracy tropes (e.g., elite capture, false flags)
- Dismissal of opposing media as "bamboozled" or corrupt
- Echo-chamber reinforcement and filter-bubble logic
- Recruitment through self-help branding (coaching, courses)
- Hijacking of personal struggles (identity, dating, success)
- Tactical repetition of emotionally loaded language
- False science/scientific authority references
- Presentation of critique as existential threat to the West

Key Concepts/Narratives

- Alt-right
- Manosphere
- Authoritarian masculinity
- Parasocial intimacy
- BITE model of authoritarian control
- Influence Continuum
- Filter bubbles
- Conspiratorial public
- Traditional gender roles
- Cultural Marxism (implied)
- Ideological grooming
- Emotional cocooning in audio formats
- Gatekeeping and community boundary policing
- Victimhood narrative (of men, masculinity, West)
- Anti-LGBTQ sentiment
- Post-truth epistemology
- Alt-lite
- Alt-right
- APIs (Application Programming Interfaces)
- Authoritarian control

- Behavior control
- BITE model
- Black-and-white thinking
- Capitalism
- Conspiratorial narratives
- Conservative ideologies
- Cult tactics
- Cult-like rhetoric
- Digital masculinity
- Digital media literacy
- Disinformation
- Echo chambers
- Emotional control
- Far-right ideologies
- Fear mongering
- Filter bubbles
- Gatekeeping
- Ging, Debbie
- Hassan, Steven
- Hyper-intimacy
- Ideological radicalisation
- Influence Continuum
- Information control
- Intimacy effect (human emotional intimacy effect)
- Jones, Alex
- Masculine identity
- Misinformation
- Online radicalisation
- Parasocial connection
- Political propaganda
- Posthumus, Bram
- Psychological manipulation
- Recommendation algorithms
- Rhetorical strategies
- Right-wing media
- Robertson, Andy
- Self-reinforcing cycles
- Shapiro, Ben
- Social media manipulation
- SDIOs
- Tate, Andrew
- Thought control
- Toxic masculinity

- Traditional gender roles
- Us-versus-them rhetoric
- Voyant (text analysis tool)

Tech Platforms/Tools

- Podcasts (as ideological media)
- Rumble
- SoundCloud
- Twitter/X
- TikTok (mentioned in Chapter 13; relevant here in dissemination)
- YouTube (inferred in Tate's ecosystem)
- Voyant tools
- APIs (as enablers of echo chambers and content curation)
- Recommendation algorithms

References

Acheson, R., and M. Papadima. 2023. The search for identity: Working therapeutically with adolescents in crisis. *Journal of Child Psychotherapy* 49, no. 1: 95–119. https://doi.org/10.1080/0075417X.2022.2160478.

Bellas, Athena, and Jodi McAlister. 2023. Let me take care of you: Domestic caretaking fantasies in boyfriend experience audio erotica. *Porn Studies* 10, no. 3: 319–333. https://doi.org/10.1080/23268743.2023.2220721.

Bull, M., and L. Back. 2003. Introduction: Into sound. In *The Auditory Culture Reader,* eds. M. Bull and L. Black, 1–18. Oxford: Berg.

Dowling, David O., Patrick R. Johnson, and Brian Ekdale. 2022. Hijacking journalism: Legitimacy and metajournalistic discourse in right-wing podcasts. *Media and Communication* 10, no. 3: 17–27. https://doi.org/10.17645/mac.v10i3.5260.

Euritt, Alyn, and Anne Korfmacher. 2022. 'And if we don't stop him, I don't know who will': Recording intimacy in my dad wrote a Porno.' *Porn Studies* 9, no. 2: 190–207. https://doi.org/10.1080/23268743.2021.1978311.

Fleet, Robert. 2022. Hate the player, not the game: Why did the Christchurch shooter's video look like a game? In *Rethinking Social Media and Extremism*, eds. Shirley Leitch and Paul Pickering, 65–86. Canberra, Australia: ANU Press. http://ebookcentral.proquest.com/lib/deakin/detail.action?docID=7023487.

Ging, D. 2019. Alphas, betas, and incels: Theorizing the masculinities of the manosphere. *Men and Masculinities* 22, no. 4: 638–657.

Grossman, M. 2017, 21 September. *Understanding Youth Resilience to Violent Extremism: A Standardised Research Measure: Final Research Report*, eds. M. Ungar, J. Brisson, V. Gerrand, K. Hadfiield, and P. Jefferies. https://search.ebscohost.com/login.aspx?direct=true&db=cat00097a&AN=deakin.b3995809&site=eds-live&scope=site.

Hassan, S.A. 2020. *The BITE Model of Authoritarian Control: Undue Influence, Thought Reform, Brainwashing, Mind Control, Trafficking and the Law* (Doctoral dissertation, Fielding Graduate University).

Hermansson, Patrik, David Lawrence, Joe Mulhall, and Simon Murdoch. 2020. *The International Alt-Right: Fascism for the 21st Century?* Routledge Studies in Fascism and the Far Right. Abingdon, Oxon; New York, NY: Routledge.

Hern, A. 2015, September 4. Who runs Hollywood? Google has an answer, but it's not a good one. *The Guardian*. https://www.theguardian.com/technology/2015/sep/04/who-runs-hollywood-google-search-direct-answer-antisemitic

Hyzen, Aaron, and Hilde Van den Bulck. 2021. 'The most paranoid man in America': Alex Jones as celebrity populist. *Celebrity Studies* 12, no. 1: 162–166. https://doi.org/10.1080/19392397.2019.1691756.

Korfmacher, Anne. 2020. Reviewing pornography: Asserting sexual agency on girls on porn. *Gender Forum* 77: 1–14.

Llinares, Dario, Neil Fox, and Richard Berry. 2018. Introduction: Podcasts and podcasting – parameters of a new aural culture. In *Podcasting: New Aural Cultures and Digital Media,* eds. Dario Llinares, Neil Fox, and Richard Berry, 1–14. Cham: Springer.

Lyons, M.N. 2017. Ctrl-alt-delete: The origins and ideology of the alternative right. *Political Research Associates* 20. https://politicalresearch.org/sites/default/files/2019-05/Lyons_CtrlAltDelete_PRINT.pdf

Madsen, Virginia, and John Potts. 2010. Voice-cast: The distribution of the voice via podcasting. In *Voice: Vocal Aesthetics in Digital Arts and Media*, eds. Norie Neumark, Ross Gibson, and Theo van Leeuwen, 33–60. Cambridge, MA: MIT Press.

Main, Thomas J. 2018. *The Rise of the Alt-Right*. Brookings Institution Press. https://www.jstor.org/stable/10.7864/j.ctt1vjqnxx.

Marwick, A.E., and R. Lewis. 2017. Media manipulation and disinformation online. *Data & Society Research Institute*. https://apo.org.au/node/135936.

Menzie, L. 2022. Stacys, Beckys, and Chads: The construction of femininity and hegemonic masculinity within incel rhetoric. *Psychology and Sexuality* 13, no. 1: 69–85. https://doi.org/10.1080/19419899.2020.1806915.

Miller, Lisa. 2023, March 13. Tate-pilled: What a generation of boys have found in Andrew Tate's extreme male gospel. *New York Magazine*. https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=00287369&v=2.1&it=r&id=GALE%7CA741580784&sid=googleScholar&linkaccess=abs.

Nawaz, M.S., Khan, S.U.R., Hussain, S., and Iqbal, J. 2023. A study on application programming interface recommendation: State-of-the-art techniques, challenges and future directions. *Library Hi Tech* 41, no. 2: 355–385. https://doi.org.ezproxy-f.deakin.edu.au/10.1108/LHT-02-2022-0103.

Neiwert, D. 2017. *Alt-America: The Rise of the Radical Right in the Age of Trump*. Verso Books.

Pettman, Dominic. 2017. *Sonic Intimacy: Voice, Species, Technics (or, How To Listen to the World)*. Stanford, CA: Stanford University Press.

Peukert, Christian, Ananya Sen, and Jörg Claussen. 2023. The editor and the algorithm: Recommendation technology in online news. *Management Science* 1–16.

Phillips, W., and R.M. Milner. 2017. *The Ambivalent Internet: Mischief, Oddity, and Antagonism Online*. Cambridge, UK: Polity Press.

Piper, Melanie. 2015. Little big dog pill explanations: Humour, honesty, and the comedian podcast. *Philament* 20: 41–60.

Robson, M. 2023. *Sound, Self and Crisis: Mapping the Affective Dimensions of Podcast Media. Open Access Te Herenga Waka-Victoria University of Wellington* (Thesis). https://doi.org/10.26686/wgtn.22564555.

Rodero, Emma, and Ignacio Lucas. 2021. Synthetic versus human voices in audiobooks: The human emotional intimacy effect. *New Media & Society* 1–19. https://doi.org/10.1177/14614448211024142.

Ross, Andrew S., and Aditi Bhatia. 2019. #secondcivilwarletters from the front: Discursive illusions in a trending twitter hashtag. *New Media & Society* 21, no. 10: 2222–2241. https://doi.org/10.1177/1461444819843311.

Salojärvi, V., E. Palonen, L. Horsmanheimo, and R.M. Kylli. 2023. Protecting the future 'US': A rhetoric-performative multimodal analysis of the polarising far-right YouTube campaign videos in Finland. *Visual Studies* 1–16.

Speakman, B., and M. Funk. 2020. News, nationalism, and hegemony: The formation of consistent issue framing throughout the U.S. Political Right. *Mass Communication and Society* 23, no. 5: 656–681. https://doi.org/10.1080/15205436.2020.1764973.

Spinelli, Martin, and Lance Dann. 2019. *Podcasting: The Audio Media Revolution*. New York, NY: Bloomsbury.

Stankievech, Charles. 2007. From stethoscopes to headphones: An acoustic spatialization of subjectivity. *Leonardo Music Journal* 17: 55–59. https://doi.org/10.1162/lmj.2007.17.55.

Starbird, K., A. Arif, and T. Wilson. 2019. Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction* 3(CSCW): 1–26.

Subrahmanyam, K., and D. Šmahel. 2011. Constructing identity online: Identity exploration and self-presentation. In *Digital Youth. Advancing Responsible Adolescent Development*. New York, NY: Springer. https://doi.org/10.1007/978-1-4419-6278-2_4.

Sunderland, J. 2023. Fighting for masculine hegemony: Contestation between Alt-Right and white nationalist masculinities on Stormfront. *Men and Masculinities* 26, no. 1: 3–23.

Teply, Aundy L. 2023. *Undue Influence and Destructive Cults in the Digital Age: Analyzing the BITE Model for the Age of Destructive Internet Groups*. M.L.S., United States – Ohio: The University of Toledo. https://www.proquest.com/docview/2856264783/abstract/19257C89217141FAPQ/1.

Tulley, Christine. 2011. IText reconfigured: The rise of the podcast. *Journal of Business and Technical Communication* 25, no. 3: 256–275.

Wescott, Stephanie, Steven Roberts, and Xuenan Zhao. 2023. The problem of anti-feminist 'manfluencer' Andrew Tate in Australian Schools: Women teachers' experiences of resurgent male supremacy. *Gender and Education* 1–16. https://doi.org/10.1080/09540253.2023.2292622.

Woolley, D., and J. Luger. 2023. The deviant leisure of gym bodies, militarized branding and fascistic creeps. In *Deviant Leisure and Events of Deviance: A Transgressive Compendium*, 143–172. Cham: Springer International Publishing.

Woolley, Samuel C. 2022. Digital propaganda: The power of influencers. *Journal of Democracy* 33, no. 3: 115–129. https://doi.org/10.1353/jod.2022.0027.

Yilmaz, Ihsan, Shahram Akbarzadeh, and Galib Bashirov. 2023, September 10. Comprehending strategic digital information operations (SDIOs). *Populism & Politics (P&P)*. European Center for Populism Studies (ECPS). https://doi.org/10.55271/pp0024.

15

FUTURE DIRECTIONS IN STRATEGIC DIGITAL INFORMATION OPERATIONS AND WARFARE

Ihsan Yilmaz

A Comprehensive Understanding of Strategic Digital Information Operations

This book has undertaken an extensive exploration of SDIOs, offering a novel framework to understand and analyze the digital manipulation by state and non-state actors. The chapters collectively address the theoretical, methodological, and empirical dimensions of SDIOs, providing insights into their impact on politics, society, and governance. This work fills a critical gap in the existing literature by not only examining the political implications of SDIOs but also highlighting their sociological, psychological, and technological ramifications. Through diverse methodologies and global case studies, the book advances the scholarly understanding of SDIOs and underscores their relevance to contemporary political and social discourse.

This book makes a contribution to the literature by introducing SDIOs as a comprehensive framework that unites political, sociological, psychological, and technological dimensions of digital manipulation. It demonstrates the global relevance of SDIOs by analyzing their application across diverse contexts, from the authoritarian strategies of state regimes to the digital tactics of extremist movements and democratic societies. By examining the intersection of state and non-state actors, the book reveals how their digital strategies both converge and diverge, offering insights into the complexity of modern information warfare. Additionally, it advances the understanding of how digital platforms drive emotive political mobilisation, reshape intergroup dynamics, and normalise divisive narratives, underscoring their transformative impact on societal cohesion and politics worldwide. Practically, the book offers insights for policymakers, scholars, and civil society actors. It

DOI: 10.4324/9781003628088-20
This chapter has been made available under a CC-BY-NC-ND 4.0 license.

underscores the need for robust digital literacy programs, international cooperation to counter transnational manipulation, and regulatory frameworks that ensure transparency and accountability in digital platforms.

In the introduction chapter, we presented the concept of SDIOs, outlining their tactics and practices and elucidating the primary political goals of both state and non-state actors in deploying SDIOs domestically and internationally. We argued that SDIOs offer a valuable framework for discussing all forms of digital manipulation orchestrated by these actors. While existing literature has examined the military-political impacts of SDIOs, there is a significant gap in understanding their influence on societal issues such as emotive political mobilisation, intergroup relations, social cohesion, trust, and emotional resonance among target audiences. This book addresses this new dimension, extensively exploring these societal impacts across various chapters.

In our coverage of the SDIOs' impact on elections (Part 1), our contributors shed light on utilising digital space for electoral purposes. As multiple social media platforms have provided an exceptional opportunity for democratic politics to promote their agenda and run more successful electrical campaigns, they have also assisted political leaders and actors in shaping and influencing online discourse. While the general role of social media in modern political parties has been studied, the role of forming and reshaping political discourse along populist lines and utilising dis/misinformation for political purposes has been less explored.

The first part offers a comprehensive understanding of SDIOs in electoral contexts. First, the two chapters, using the case studies of Pakistan and Nigeria, show that digital platforms offer both advantageous and disadvantageous conditions for democracy. These platforms can allow major political parties to engage with the electorate and increase their democratic participation. However, state and non-state actors can and do also use these platforms to spread misinformation. For example, in both cases, social media was used by political parties and non-electoral actors to vilify opposition, manipulate opinion, and disseminate false narratives. The fact that digital platforms serve as vehicles for democratic participation and sources of false information emphasises how complicated their influence on contemporary politics is. Responding to this duality requires a balanced strategy that takes advantage of digital engagement while putting protections against manipulation and misinformation in place. Policymakers and academics should negotiate more effectively the difficulties presented by digital platforms in the political sphere and ensure they are used to enhance democratic processes.

Furthermore, the analyses in the book illustrate the clear link between SDIOs and the amplification of populist and identity politics. In Nigeria, for instance, politicians like Peter Obi used sophisticated digital campaigns to frame 2023 as a generational battle and appeal to the youth. Similarly, in

Pakistan, political parties consistently utilised digital platforms, and information manipulation such as circulating dis/misinformation, to present themselves as the people's voice while condemning opponent political parties as corrupt and impure. This demonstrates that SDIOs, operatiationalising the affordances of digital platforms, have the potential to oversimplify the electoral arena into the binaries of populism ("us" vs. "them"), diverting attention from crucial issues related to the well-being of the people. Moreover, the operationalisation of identity politics through SDIOs fosters further division. The Nigerian case study illustrates how electoral actors can garner support by manipulating religious, ethnic, and generational identities. This form of divisive politics affects social cohesion and intergroup relations, thereby leading to a more fragmented society.

Notably, the findings of both chapters underscore the presence of non-electoral actors in the digital sphere. This is a significant discovery, aligning with one of the larger themes of this book: SDIOs are not limited to state and electoral actors. The results indicate a major shift in the sources of political influence, with non-electoral players increasingly leading digital operations. In Pakistan, non-electoral actors play a crucial role in party propaganda, often taking the lead in digital influence efforts. This influence is substantial and cannot be overlooked. In Nigeria, online platforms provide marginalised populations a voice, enabling them to claim political power. This shift underscores the changing terrain of political communication and the need to understand the many parties participating in and benefiting from SDIOs.

The second part of this book comprehensively examines how conspiracy theories are disseminated on various digital platforms as part of the SDIOs of both state and non-state actors. Our contributors demonstrate how conspiracy theories can be used as a form of political and social control. Using the spread of conspirational discourse on X (formerly Twitter) during the 2023 Maui wildfires as a case study, the first chapter in this part introduces two concepts – "conspirational publics" and "conspirational canon" to explain the networks, communities, and origins of conspiracy theories enacted on digital platforms. By applying this conceptualisation to an empirical study, the authors addressed a gap in digital information operation literature, answering the question of why some conspiratorial narratives are ephemeral and why others remain pervasive in public discourse. This undertaking provides a broader analysis of the fertile sociopolitical ground from which conspiratorial movements grow. The authors discovered that social media platforms amplify conspiracy theories through algorithmic processes. In-built features like trending lists and algorithmic amplification, which treat institutional knowledge and fringe theories equally, contribute to the visibility and perceived legitimacy of conspiratorial content. This problematic amplification helps conspiracy theories gain disproportionate attention.

Hence, conspiracy theorists actively use social media affordances to spread their narratives, engaging in collective sensemaking and dis/misinformation production to undermine political opponents through the strategic spread of conspiratorial narratives.

In the second chapter dedicated to conspiracy theories, the utilisation of conspiracy theories as a means of political manipulation and control over society was studied in the case of Egypt, furthering research on this phenomenon, which has been disproportionately studied in the Western context. The chapter extensively investigates the key conspiracy theories produced and disseminated by the Egyptian government after the Russian invasion of Ukraine, with a focus on explaining how the regime has been using digital technologies to disseminate these narratives. The narrative focuses on the war in Ukraine, demonstrating the way in which a distinct geopolitical event can be implicated in conspiracy theories. The contributors argue that widespread digital technologies have assisted authoritarian regimes in promoting their agendas through systematic conspiracy narratives made by various media affiliated with them. Within such a climate of conspiratorial thought dissemination, the Russian war against Ukraine offers a fertile ground for the Egyptian propaganda apparatus to construct complex conspiracy narratives.

The contributors of Part 2 collectively describe the larger impacts and harms of conspiracy theories on democracy and social integration, demonstrating how conspiracy theories undermine social cohesiveness by polarising communities and establishing a culture of distrust. The normalisation of hate discourses and the strategic dissemination of disinformation jeopardise the credibility of democratic systems and weaken confidence in political structures. This shared understanding emphasises the necessity for actions to combat the negative repercussions of conspiratorial discourses on democracy and beyond.

Part 3 of this book sheds light on the use of digital spaces by authoritarian regimes to impose control and expand domination over society across various regions, focusing on Thailand, Turkey, India, and Hungary as case studies. In the Thailand case study chapter, the author highlights the significant role of state actors in conducting IO. SDIOs in Thailand are found to involve three stages: *Learning, Adapting,* and *Normalising*. The study shows that state actors, especially the military, have evolved into more advanced digital actors by acquiring sophisticated tools and building networks with non-state actors, including pro-regime media outlets and royalist civic groups. Political parties, such as the Palang Pracharath Party (PPRP), play a pivotal role in SDIOs, further blurring the boundaries between state and non-state propaganda. The Thai case study highlights how a powerful digital Propaganda Model has the potential to not only jeapordise freedom of expression but also hamper democratic development.

The following chapter studies the Turkish government's domestic digital IO on X (Twitter), focusing on the AK Party's use of trolls, bots, and hackers to shape public opinion and instigate emotionally charged political mobilisation. This includes building the ideological concept of a "New Turkey," cultivating Erdogan's personality cult, and targeting opposition figures as internal "others." These operations are designed to provoke a spectrum of emotional responses – primarily anger, fear, and pride – to manipulate narratives and legitimise repressive governance. The chapter reveals how digital propaganda in Turkey dehumanises dissenting voices (such as the Gezi protesters) and undermines democratic norms, press freedom, and civil liberties. The Turkish experience is presented as emblematic of broader global trends in digital information manipulation, demonstrating how digital authoritarianism erodes social cohesion and distorts democratic discourse.

In the next chapter, the contributors critically examine how the Modi-led BJP government has transformed the country into a digital authoritarian state through a comprehensive and institutionalised strategy of SDIOs. The government employs censorship laws, internet shutdowns, disinformation campaigns, troll armies, and emotionally charged Hindu nationalist narratives to suppress dissent and shape public opinion. State-aligned media reinforce official narratives, while platforms like Twitter, Facebook, and WhatsApp are leveraged to disseminate propaganda and harass critics. Through case studies of the farmers' protests, the Delhi riots, the COVID-19 "infodemic," and electoral disinformation in 2019 and 2024, the chapter illustrates how the state uses digital tools to criminalise protest, scapegoat minorities (especially Muslims), and dominate the information space. The cumulative effect of these strategies has severely impacted civil liberties, press freedom, democratic discourse, and social cohesion, showcasing how digital control can entrench authoritarian governance in a formally democratic framework.

Hungary is the case study in the following chapter, and the authors examine how the ruling party under Prime Minister Viktor Orbán exerts control over the media using three main mechanisms: *legislative intervention, financial manipulation,* and *political pressure*. Specific strategies detailed in this discussion include legal frameworks being altered to enable institutions to limit media plurality and financial pressure tactics, including acquisitions by pro-Orbán allies, to skew the media environment in favor of the government. Simultaneously, left-wing journalists and opposition figures face systematic defamation and attacks on their character. These pressures have marginalised critical voices and created a hostile environment for independent journalism. The study also highlights the propagation of conspiracy theories and the demonisation of the opposition as central strategies of the ruling party, thus compromising press freedom and democratic values in Hungary.

The collective knowledge presented by the contributors in this part illustrates that the developing digital domain has not offered the anticipated

avenues for bypassing traditional authoritarian constraints. Instead, it has opened opportunities for digital authoritarianism as a new form of control. As digital media becomes increasingly inseparable from society and citizens' daily lives, authoritarian governments have effectively tightened their grip on society by orchestrating carefully planned SDIOs. As such, rather than supporting democratisation, digital technologies have frequently enabled more sophisticated and widespread forms of political control.

Looking beyond domestic digital authoritarianism, Part 4 of the book examines SDIOs in the context of transnational dynamics. The three chapters in this part demonstrate that authoritarian governments employ SDIOs to target not only dissenters living within national boundaries but are also increasingly directed at dissidents living abroad. The first chapter examines the strategies employed by the Iranian regime to spread online disinformation and describes how SDIOs have been deployed as tools for controlling and dividing society, and discrediting influential opponents, both at home and abroad. During the 2022 "Women, Life, Freedom" protests, amid a growing legitimacy crisis, the regime utilised major falsehoods online to undermine influential dissidents and prevent the formation of an effective opposition. The study focused on the "Big Lie" propaganda technique in politics, highlighting how these lies are predominantly crafted in the digital realm by state-affiliated online media and pro-regime social media accounts. The Big Lie studied in this chapter aims to persuade Iranians that voices of opposition are untrustworthy and incapable of offering a viable alternative to the Islamic Republic. Two main reasons for this strategy were identified. First, social media has proven to be a fertile ground for the rapid and widespread dissemination of falsehoods. Second, the Islamic Republic has faced a significant legitimacy crisis, marked by four nationwide anti-regime protests from 2009 to 2022. To combat this, the regime has launched systemic disinformation campaigns to discredit dissidents and undermine public aspirations for change. The humiliation of opponents is central to disqualifying the credibility of influential dissidents, often through character assassination together with conspiracy theories. The research noted that the Iranian regime, on the back of the Big Lie conspiracy theory, targeted various Iranians living abroad as well. This targeting had the larger message of shunning life outside of Iran, attaching the well-being of Iranians to the Islamic regime only.

The next chapter in this part presented Russia's digital operations that seek to increase the country's influence in the Western Balkan region, especially in countries like Serbia. Authors found that Russia's disinformation efforts have been implicated in various events, including the Brexit referendum and the 2016 US presidential election. In Europe, the Kremlin aims to undermine Euro-Atlantic integration and Western unity, viewing a disunited West as advantageous to Russian interests. The Western Balkans region

has become a battleground for geopolitical influence, with the EU and the US vying for closer ties while Russia and China seek to expand their influence. The invasion of Ukraine in 2022 has heightened tensions in Europe and spurred increased defense spending and NATO expansion. However, with the exception of Montenegro, the Western Balkans remain outside NATO's reach. This has presented an opportunity for Moscow, which has significantly increased its involvement in the Western Balkans, especially Serbia, over the past decade. Adopting a multifaceted strategy, Russia expands its influence by emphasising cultural affinity, leveraging Orthodox religion as a shared identity marker, disseminating pro-Russian narratives and propaganda, and enacting disinformation campaigns to prevent Western Balkan states from joining NATO and the EU.

The final chapter in this part compared the use of digital technologies to facilitate transnational authoritarianism in Turkey and India. The authors examined SDIOs employed by Turkey's AKP and India's BJP governments. These operations include state-sponsored disinformation campaigns, censorship, intimidation of influential netizens, and legislation manipulation. The study demonstrated that both the Indian and Turkish governments use SDIOs as a key tool in their authoritarian populist governance to build legitimacy, suppress criticism, and evade accountability both domestically and transnationally. Various actors, including government entities, ruling party IT cells, trolls, and national and global pro-BJP, pro-AKP, pro-Hindutva, and Islamist groups, as well as genuine followers, champion these operations and create a far-reaching network of state and non-state actors. The SDIOs consist of censorship campaigns, disinformation campaigns (including fake news and half-truths), and pro-government and ideological propaganda. The study found that SDIOs are facilitated by anti-democratic laws and regulations, often in cooperation with transnational and domestic pro-government actors such as pro-government diaspora groups, trolls, politicians, journalists, transnational government organisations, and private-sector companies. In this context, Indian and Turkish diasporas, as well as journalists and politicians in other countries are perceived as threats to the nation (India or Turkey), and become key targets of SDIOs. The freedom and safety of these individuals and collectives are compromised in these circumstances, while the authoritarian influence of these regimes extends within and beyond their borders.

The contributors to this part on transnational dynamics in the context of SDIOs add significant theoretical value to our knowledge of contemporary totalitarianism and its digital manifestations. One notable theoretical contribution is the clarification of authoritarian governments' global reach via SDIOs. Together, the chapters highlight how authoritarian governments use SDIOs to impose authority over national and international realms, broadening the reach and severity of political oppression in authoritarian settings.

National boundaries become less significant in the context of political coercion and control enacted in digital spaces.

Another important finding from these chapters finds that state actors leverage SDIOs as a form of sharp power to increase their influence in a specific region. The case of Russia, in this regard, is a prime example. Russia's strategic employment of SDIOs in Serbia illustrates the complex character of these operations, in which digital tools are utilised both defensively and aggressively to expand influence. The manipulation of Serbian media serves numerous aims, including strengthening pro-Russian attitudes, undermining Western influence, and disrupting regional political cohesiveness. Russia effectively reshapes public perception and political discourse by inundating the media with pro-Kremlin narratives, producing a more favorable climate for its geopolitical goals. As such, it can be concluded that the SDIOs do not merely assist state actors in suppressing dissent but also allow them to project their power and ideology beyond their frontiers.

In the last part (Part 5), authors evaluated non-state actors and extremism, studying the differences between state and non-state actors in SDIOs, finding out that although state actors demonstrate more sophistication and strategic complexity, non-state actors are characterised by their opportunistic nature and adaptability. Understanding these differences is essential for developing effective strategies to counter malicious activities in the digital domain. Accordingly, state actors engage in more coordinated and strategic IO with global reach and significant geopolitical impact, focusing on disinformation campaigns and targeting critical infrastructure. Non-state actors, while increasingly adopting cyber capabilities, typically have limited capacity unless acting as proxies for states. Their operations are marked by financial motivations, ransomware attacks, and a degree of unpredictability due to diverse motivations. The intersection of state and non-state actors in cyber operations presents a complex and dynamic terrain in digital information warfare. Non-state organisations have increasingly adopted offensive cyber capabilities to further their strategic objectives, making countermeasures more challenging. Powerful non-state armed groups often act on behalf of a state, as in performing proxy operations, offering plausible deniability.

We also studied the use of SDIOs by Alt-Right Ideology to promote masculinity and gender discrimination. The authors examined *The Alex Jones Show*, *Tate Speech*, and *The Ben Shapiro Show*, positioning them as podcasts with varying degrees of proximity to the alt-right ideology, demonstrating that rather than being explicitly alt-right, these podcasts operate as conduits that normalise and desensitise their predominantly young male audiences to alt-right ideas, potentially serving as gateways to further radicalisation. Our analysis also revealed a spectrum of alt-right ideological usage across these podcasts, as well as a range of tactics from the BITE model employed to exert undue influence on their listeners. The episodes analyzed within *The*

Alex Jones Show and *Tate Speech* were weighted heavily toward the authoritarian/destructive side of the Influence Continuum, while *The Ben Shapiro* episode framed similar ideological concepts in a less authoritarian manner. This contributes to a culture of misogyny and male dominance, fostering an environment conducive to the acceptance of alt-right ideologies. *Tate Speech* also targets men who feel victimised not by these movements but by promoting a self-sufficient form of masculinity.

Part 5 contributes to the literature as a result of the synergy between the two chapters. This book has extensively noted that SDIOs have been understudied in extant literature, with a few studies only focusing on state actors. As such, the significant task of this book was to clearly introduce and delineate SDIOs in the context of non-state actors. We presented the characteristics of non-state actors' SDIOs and then compared them with state actors' digital operations. Non-state actors, such as extremist organisations and ideologically driven movements, were identified as having greater flexibility and may swiftly adjust to changing conditions. Their activities are characterised by financial goals, opportunistic ransomware assaults, and an element of unpredictability resulting from their varied motivations and decentralised structures. These players frequently lack the vast resources of state actors, but they compensate with creative and fluid methods for digital operations.

Additionally, the analysis of alt-right podcasts added another dimension to the study of SDIOs as employed by non-governmental actors. Here, it was seen that influential private individuals, such as podcast show hosts, can normalise overtly extreme ideas, especially those pertaining to hyper-masculinity. This highlights the feasibility of SDIOs to private individuals and groups (not aligned with national governments), who can potentially employ them to propagate extremist ideologies and shape public opinion. Collectively, both chapters in this part expand the concept of SDIOs beyond state-centric frameworks, demonstrating the fluid nature of non-state actors in the digital sphere.

Future Directions in Digital Information Warfare

The exploration of SDIOs in this book offers a comprehensive view of the digital manipulation. However, the dynamic and fast-paced nature of digital technologies means that the study of SDIOs must remain adaptive and forward-looking. This part synthesises the key insights from the book and proposes future directions for research, policy, and societal engagement to better understand and counter digital information warfare.

The rapid advancement of technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics is reshaping the SDIOs. Future research should explore how these innovations are leveraged to craft highly targeted and sophisticated campaigns. AI-driven bots can now simulate

human-like interactions, while deepfake technology enables the creation of highly convincing fake media, raising new ethical and operational challenges. These technologies allow for the manipulation of visual and audio content, making disinformation campaigns more effective and harder to detect. Understanding how these tools are deployed at scale will be essential for predicting and responding to future trends in digital manipulation.

Moreover, the integration of predictive analytics and sentiment analysis into SDIOs allows for the real-time adaptation of strategies based on audience reactions. This capability means that campaigns can evolve dynamically, increasing their effectiveness and minimising their detection. Researchers and policymakers need to anticipate these shifts by examining the relationship between emerging technologies and human vulnerabilities, as well as developing countermeasures that can keep pace with these advancements.

The growing intersection between state and non-state actors in digital information warfare presents a complex challenge. State actors often rely on non-state proxies, such as private militias, ideologically aligned groups, or even cybercriminal networks, to execute disinformation campaigns while maintaining plausible deniability. This collaboration creates a multilayered network of influence that complicates attribution and accountability.

Future research should investigate the mechanisms of these partnerships, including resource sharing, the outsourcing of cyber capabilities, and the strategic use of non-state actors to amplify state narratives. For instance, how do states indirectly fund or provide technological support to such groups? What incentives drive non-state actors to align with state agendas? Addressing these questions will shed light on the covert dynamics of SDIOs and the ways in which state and non-state actors mutually benefit from such collaborations. Additionally, studies should examine how non-state actors independently exploit digital platforms to further their own agendas, including financial gain, ideological propagation, and political disruption. Understanding this relationship will provide a more complex view of the digital battlefield and help identify vulnerabilities in the information ecosystem that these actors exploit.

The transnational nature of SDIOs has blurred the lines between domestic and international operations, creating a global battlefield for digital influence. Authoritarian regimes increasingly export their disinformation tactics to influence foreign populations, while democratic nations also grapple with their own use of SDIO-like strategies. This globalisation raises questions about sovereignty, accountability, and the ethical implications of cross-border information manipulation. Future research should address the geopolitical ramifications of SDIOs, including how they influence alliances, reshape regional power dynamics, and challenge traditional notions of international relations. For instance, how do regimes like Russia and China leverage SDIOs to undermine Western democracies while bolstering their own geopolitical

agendas? Conversely, how do democratic states balance the use of digital tools for countering disinformation without compromising their own values of transparency and free speech? Additionally, studies should explore the role of international organisations and coalitions in regulating transnational SDIOs. Can global frameworks be developed to hold actors accountable, or will national interests continue to undermine collective efforts? By examining these questions, future research can contribute to a more coordinated and effective global response to digital information warfare.

The role of SDIOs in eroding democratic institutions and polarising societies has been a central theme of this book. However, the conversation must now shift toward identifying strategies that can enhance democratic resilience in the face of these threats. This includes understanding how different societies respond to disinformation and what factors contribute to their vulnerability or resistance. Future studies should focus on the effectiveness of interventions such as media literacy campaigns that empower citizens to identify false information, algorithmic transparency initiatives that reduce the amplification of harmful content, and policy reforms that address the regulatory gaps in digital platforms. For example, what role do local cultural and political contexts play in shaping the success of these interventions? How can these measures be tailored to diverse audiences while maintaining universal principles of fairness and equity? Additionally, there is a pressing need to explore the role of civil society organisations in countering SDIOs. Grassroots initiatives, fact-checking collaborations, and community-based digital literacy programs have shown promise in building resilience. Future research should document these efforts and identify best practices that can be scaled up to create broader societal impact.

While this book has highlighted the activities of non-state actors, future research should look more deeply at their dynamic roles and motivations. Non-state actors, ranging from extremist groups to ideologically driven collectives and influential individuals, have demonstrated remarkable adaptability in leveraging digital platforms for their goals. They often have less resources than state actors but compensate with agility, innovation, and a keen understanding of their audiences. One area of interest is the increasing use of blockchain technologies and decentralised platforms by non-state actors to evade censorship and maintain anonymity. How do these tools change the dynamics of digital information warfare? Additionally, studies should explore the impact of non-state actors on international conflicts, examining cases where their activities exacerbate tensions or influence diplomatic outcomes. Understanding the intersection of non-state actors with private corporations, such as tech firms or data brokers, also warrants attention. How do these partnerships shape the strategies and effectiveness of non-state SDIOs? Expanding the scope of research to include these dimensions will provide a more holistic understanding of the non-state terrain in digital warfare.

While this book provides a snapshot of SDIO strategies and impacts, there is a need for longitudinal studies that track their long-term effects on societies. These studies should examine how sustained exposure to disinformation, conspiracy theories, and manipulative narratives reshapes public opinion, political engagement, and social trust over time. For example, how do communities recover from the divisive impacts of SDIOs once the immediate threat has passed? What role do reconciliation efforts and truth commissions play in rebuilding trust? Additionally, longitudinal research could explore the generational differences in susceptibility to digital manipulation, offering insights into how younger and older audiences engage with online content differently. These studies would provide valuable data for policymakers, educators, and civil society organisations seeking to address the root causes of societal polarisation, create tailored solutions for improving resilience to digital manipulation across all sections of society, and strengthen democratic institutions in the digital age.

Finally, the complexity of SDIOs requires a multidisciplinary approach that integrates insights from political science, sociology, psychology, computer science, and media studies. Future research should prioritise collaborations across these fields to develop innovative methodologies and comprehensive frameworks for analyzing and countering digital information warfare. For example, how can computational tools like machine learning be combined with qualitative methods to uncover the hidden networks and narratives driving SDIOs? What role can psychological theories of persuasion and influence play in designing more effective countermeasures? By fostering interdisciplinary dialogue, the academic and policy communities can generate more robust and actionable insights to address the challenges of SDIOs.

Funding: This work was supported by Australian Research Council [Grant Number DP230100257] and Gerda Henkel Foundation [Grant Number AZ 01/TG/21].

INDEX

Note: Page numbers in *italic* indicate a figure, and page numbers in **bold** indicate a table on the corresponding page.

adapting 112–115
ad hoc publics 71–72, 78
advertising 118
affordances, social media 88–92
AK Trolls 127–128
Alex Jones Show, The 260–261, *261*
algorithmic amplification 1, 69–70, 280
alt-right ideology 254–256, 269–272; *The Alex Jones Show* 260–263; *The Ben Shapiro Show* 267–269; cult tactics and SDIOs 257–259; digital dissemination 257; methodological framework for analyzing masculinity in podcasts 259–260; online influence operations 256–257; *Tate Speech* 263–267
appropriation of emerging events 65–67, 81–82; case study 74–80; co-hashtagging as SDIO user practice 80–81; conspiratorial canon 72–73; conspiratorial publics 70–72, 73–74; methods 74; recurring tropes and continuing communities 67–68; social media architecture 68–70
Australia 220, 223–224, 244, 250, 255
authoritarian context, conspiracy theories in 87–88
authoritarianism *see* digital authoritarianism
authoritarian regimes, social media affordances for 88–92
authoritarian tendencies 159–162, 170–172; destabilising media independence through three mechanisms 162–163; financial pressure and manipulation 163–166; political pressure 166–170

Balkan countries 193–195; disinformation and its conceptual anchoring 195–197; Russian disinformation campaigns 197–204
behavior control 261–262, 266, 268
Ben Shapiro Show, The 267–269, *267*
Big Lies 21, 178–182, 183–184, 189
bots 128–129, 145–146

Canada 222, 225; Alberta Premier 262
case studies 74–75, 146–153
celebrities 184–186
censorship: of dissent 213–214; legislation 142–144
Central European countries 159–162, 170–172; destabilising media independence through three mechanisms 162–163; financial pressure and manipulation 163–166; political pressure 166–170

China 5–7, 33, 193–194, 224–226, 241
civil liberties 153–155
co-hashtagging 80–81
communalising public health crisis 150–151
communities: community practice 75–80, *78–79*; conspiratorial 72–73; continuing 67–68
comparative analysis 25–26, 37–41; content dissemination and coordination 36–37; data collection and curation 31–32; narrative alignment 34–36; new forms of social actors 26–29; Pakistan 2024 elections and digital politics 29–31; topics and discourse 32–34
consent, manufacturing 107–108; adapting 112–115; background 108–109; filters in social media era 117–120; learning 110–112; normalising 115–116; political economy of SDIOs 116–117; SDIO in Thailand 109–110
consolidation of digital authoritarianism 86–87, 100–101; authoritarian context 87–88; conspiracy theories 92–100; history and cultural background 92; social media affordances 88–92
conspiracy campaigns 145–146
conspiracy theories 12–13, 86–87, 92–101; authoritarian context 87–88; history and cultural background 92; logic of 67–68; #MauiPsyOps 75–80, *78–79*; social media affordances 88–92; and social media architecture 68–70
conspiratorial canon 72–73
conspiratorial communities 72–73
conspiratorial publics 70–72, 73–74; #MauiPsyOps as 75–80, *78–79*
content dissemination and coordination 36–37, *37*
continuing communities 67–68
co-opting diaspora organisations 216–217
coordination 36–37, *37*
COVID-19 "infodemic" (2020–2021) 150–151
critics, harassment and intimidation of 215
crushing solidarity 146–148
cult tactics 257–259
cultural background of conspiracy theories 92

data collection 31–32, **32**, 74
data curation 31–32, **32**
deep state *see* global elites/deep state
Delhi riots (February 2020) 148–150
democracy 124–126, 136–137; emotive political mobilisation on social media 130–133; organising grassroots campaigns for online manipulation 126–130; targeting opposition as internal enemies 133–135; threatened democratic discourse 153–155
destabilising media independence 162–163
diaspora 177–179, 188–189; Big Lie in Iranian regime's propaganda 181–182; Big Lies in modern politics 179–181; celebrities 181–186; co-opting diaspora organisations 216–217; methodology 182–183; political participation 56–57; prominent dissidents in diaspora 186–188; protests of 2022 183–184; surveillance 215–216, 221–223
diffusion of conspiracy theories 86–87, 100–101; authoritarian context 87–88; conspiracy theories 92–100; history and cultural background 92; social media affordances 88–92
digital affordances 66
digital authoritarianism 13–16, 86–87, 100–101; authoritarian context 87–88; conspiracy theories 92–100; history and cultural background 92; social media affordances 88–92
digital dissemination 257
digital dissonance 254–256, 269–272; *The Alex Jones Show* 260–263; *The Ben Shapiro Show* 267–269; cult tactics and SDIOs 257–259; digital dissemination 257; methodological framework for analyzing masculinity in podcasts 259–260; online influence operations 256–257; *Tate Speech* 263–267
digital information 45–47, 57–58; conceptual consideration 47–48; digital media strategic manipulation and influence in elections 50–53; disinformation and misinformation

48–50; ethno-religious politics 53–55; spatial nationalism 56–57
digital information operations *see* domestic digital information operations; strategic digital information operations (SDIOs)
digital information warfare 286–289
digital jihad 250–251
digital manipulation 134–135, 145–146
digital media 53–57; strategic manipulation and influence on elections 50–53
digital nationalism 216–217
digital parties 25–26, 37–41; content dissemination and coordination 36–37; data collection and curation 31–32; narrative alignment 34–36; new forms of social actors 26–29; Pakistan 2024 elections and digital politics 29–31; topics and discourse 32–34
digital politics 29–31
digital tools, differences in utilisation of 237–238, 251–252; background 238–241; digital jihad 250–251; global landscape 243–244; non-state actors 242–243, 244–246; Shabab social media influencers 248–250; Shabab and Somali government 246–248; state actors 241–242
directed energy weapons (DEWs) 76–78, 80–81
discourse 32–33, *33*; ephemeral feature of 73–74; threatened democratic discourse 153–155
disinformation 45–50, 57–58, 177–179, 188–189, 195–197;Big Lie in Iranian regime's propaganda 181–182; Big Lies in modern politics 179–181; campaigns 145–146, 197–204, 214–215; celebrities 181–186; conceptual consideration 47–48; digital media strategic manipulation and influence in elections 50–53; electoral 151–153; ethno-religious politics 53–55; methodology 182–183; prominent dissidents in diaspora 186–188; protests of 2022 183–184; spatial nationalism 56–57
dissemination 36–37, *37*
dissent 146–148; censorship of 213–214
dissidents 177–179, 188–189; Big Lie in Iranian regime's propaganda 181–182; Big Lies in modern politics 179–181; celebrities 181–186; methodology 182–183; prominent dissidents in diaspora 186–188; protests of 2022 183–184; transnational harassment of 219–221
domestic digital information operations 124–126, 136–137; case studies 146–153; emotive political mobilisation on social media 130–133; general characteristics 142; organising grassroots campaigns for online manipulation 126–130; targeting opposition as internal enemies 133–135

economic war 94–96
Egypt 86–87, 100–101; authoritarian context 87–88; conspiracy theories 92–100; history and cultural background 92; social media affordances 88–92
elections 10–12; India 2019 and 2024 151–153; Nigeria 2023 45–58; Pakistan 2024 29–31; Turkey 2023 134–135
emerging events, appropriation of 65–67, 81–82; case study 74–80; co-hashtagging as SDIO user practice 80–81; conspiratorial canon 72–73; conspiratorial publics 70–72, 73–74; methods 74; recurring tropes and continuing communities 67–68; social media architecture 68–70
emotional control 263, 266, 268
emotional mobilisation 130–133, 146
enduring logic of conspiracy theories 67–68
ephemeral feature of discourse 73–74
epistemology of conspiratorial communities 72–73
Erdogan, R.T. 14–15, 128–136, 211–212, 282; personality cult 132–133; promoting image of 217–218
ethical considerations 74
ethno-religious politics 53–55
ever-present public 73–74
extremism 19–21

false flags/PsyOps 74–81, 262
farmers' protest (2020–2021) 146–148
filters in social media era 117–120

financial pressure 163–166
flak 119
foreign influence operations 223–226
foreign politics, interference in 215–216

geopolitics 92–97
global elites/deep state 78, 219, 262
global landscape 243–244
goals of SDIOs 6–8
government control 142–144
grassroots campaigns 126–130
Gülen movement 132, 212–213

hackers 129–130
harassment 215, 219–221
hate 148–150
HDP 134–136
history of conspiracy theories 92
Hungary 159–162, 170–172; destabilising media independence through three mechanisms 162–163; financial pressure and manipulation 163–166; political pressure 166–170

identity-based mobilisation strategies 146
identity politics 47–50
ideology 119–120, 254–256, 269–272; *The Alex Jones Show* 260–263; *The Ben Shapiro Show* 267–269; cult tactics and SDIOs 257–259; digital dissemination 257; methodological framework for analyzing masculinity in podcasts 259–260; online influence operations 256–257; *Tate Speech* 263–267
impacts of SDIOs 1, 3, 8–11, 13–15, 17–18, 20
independence, media 162–163
India 141–142, 209–211, 226–227; case studies 146–153; digital manipulation 145–146; emotional and identity-based mobilisation strategies 146; government control and censorship legislation 142–144; internet shutdowns and social media removal requests 144–145; propaganda campaigns via state-aligned media 142; SDIOs 218–226; threatened democratic discourse 153–155; transnational SDIOs 219–226
Influence Continuum model 263, 267, 269
influence networks 221–223
influence operations: foreign 223–226; online 256–257
informational manipulation 65–67, 81–82; case study 74–80; co-hashtagging as SDIO user practice 80–81; conspiratorial canon 72–73; conspiratorial publics 70–72, 73–74; methods 74; recurring tropes and continuing communities 67–68; social media architecture 68–70
information control 262, 266, 268
information operations 237–241, 251–252, 254–256, 269–272; *The Alex Jones Show* 260–263; *The Ben Shapiro Show* 267–269; cult tactics and SDIOs 257–259; digital dissemination 257; digital jihad 250–251; global landscape 243–244; methodological framework for analyzing masculinity in podcasts 259–260; non-state actors 242–243, 244–246; online influence operations 256–257;Shabab social media influencers 248–250; Shabab and Somali government 246–248; state actors 241–242; *Tate Speech* 263–267
instability 96–97
interference in foreign politics 215–216
internal enemies 133–135
International Grains Agreement (IGA) 93–94
internet shutdowns 144–145
intimidation of critics overseas 215
Iran 177–179, 188–189; Big Lie in Iranian regime's propaganda 181–1182; Big Lies in modern politics 179–181; celebrities 181–186; methodology 182–183; prominent dissidents in diaspora 186–188; protests of 2022 183–184
issue publics 68–71

Kremlin 193–195; disinformation and its conceptual anchoring 195–197; Russian disinformation campaigns 197–204
Kurds 135

learning 110–112
legislation, censorship 142–144
local nativism 132
logic of conspiracy theories 67–68

manipulation: digital 134–135, 145–146; of digital media 50–53; electoral influence and disinformation 151–153; financial 163–166; informational 65–82; online 126–130
manufacturing consent 107–108; adapting 112–115; background 108–109; filters in social media era 117–120; learning 110–112; normalising 115–116; political economy of SDIOs 116–117; SDIO in Thailand 109–110
masculinity 254–256, 269–272; *The Alex Jones Show* 260–263; *The Ben Shapiro Show* 267–269; cult tactics and SDIOs 257–259; digital dissemination 257; methodological framework for analyzing masculinity in podcasts 259–260; online influence operations 256–257; *Tate Speech* 263–26
Maui fires of 2023 74–75
#MauiPsyOps 67, 70, 74–81, *78–79*
media 159–162, 170–172, 193–195; destabilising media independence through three mechanisms 162–163; disinformation and its conceptual anchoring 195–197; financial pressure and manipulation 163–166; political pressure 166–170; Russian disinformation campaigns 197–204; state-aligned 142; *see also* digital media; social media
Middle East 86–87, 100–101; authoritarian context 87–88; conspiracy theories 92–100; history and cultural background 92; social media affordances 88–92
misinformation 45–50, 57–58; conceptual consideration 47–48; digital media strategic manipulation and influence in elections 50–53; ethno-religious politics 53–55; spatial nationalism 56–57
mobilisation: emotional and identity-based strategies 146; political 130–133

narrative/s: against Gülen movement 135; narrative alignment 34–36, *35*
nationalism: digital 216–217; spatial 56–57
national nativism 132
networked environments, technosocial 70–72
#NewTurkey 131–132
Nigeria 45–47, 57–58; conceptual consideration 47–48; digital media strategic manipulation and influence in elections 50–53; disinformation and misinformation 48–50; ethno-religious politics 53–55; spatial nationalism 56–57
non-state actors 19–21, 237–246, 251–252; digital jihad 250–251; global landscape 243–244; Shabab social media influencers 248–250; Shabab and Somali government 246–248; and state actors 241–242
normalising 115–116

offline violence 148–150
online hate 148–150
online influence operations 256–257
online manipulation 126–130
opposition: smearing opponents abroad 217–218; targeting 133–135
organising grassroots campaigns 126–130
ownership 117

Pakistan 25–26, 37–41; content dissemination and coordination 36–37; data collection and curation 31–32; narrative alignment 34–36; new forms of social actors 26–29; Pakistan 2024 elections and digital politics 29–31; topics and discourse 32–34
performative criticality 66
personality cult 132–133
podcasts 259–260
political economy of SDIOs 116–117
political mobilisation, emotive 130–133
political parties 244–246
political pressure 166–170
politics 25–26, 37–41; Big Lies in 179–181; content dissemination and coordination 36–37; data collection and curation 31–32; diaspora political participation 56–57; interference in foreign politics 215–216; narrative alignment 34–36; new forms of social actors 26–29; Pakistan 2024 elections and digital

politics 29–31; topics and discourse 32–34; *see also* ethno-religious politics; identity politics; visibility politics
populism 45–47, 57–58; conceptual consideration 47–48; digital media strategic manipulation and influence in elections 50–53; disinformation and misinformation 48–50; ethno-religious politics 53–55; spatial nationalism 56–57
populist expertise 68–69, 80
populist tendencies 159–162, 170–172; destabilising media independence through three mechanisms 162–163; financial pressure and manipulation 163–166; political pressure 166–170
practices of SDIOs 3, 5–6, 8, 10
productive epistemology of conspiratorial communities72–73
#propaganda 107–108; adapting 112–115; background 108–109; campaigns 142; filters in social media era 117–120; learning 110–112; model 116–117; normalising 115–116; political economy of SDIOs 116–117; SDIO in Thailand 109–110
PsyOps *see* false flags/PsyOps
public health crisis 150–151

quote tweets 69

recurring tropes 67–68
repression 135
retweets 30–32, 76–77, 127, 185–188, 225
#RisingTurkey 131–132
Russia 93–94; disinformation campaigns 197–204; *see also* Kremlin

secessionism 53–55
Serbia 193–195; disinformation and its conceptual anchoring 195–197; Russian disinformation campaigns 197–204
Shabab 246–248; social media influencers 248–250
shutdowns, internet 144–145
smearing: dissent 146–148; opponents abroad 217–218
social actors, new forms of 26–29
social cohesion 124–126, 136–137, 153–155; emotive political mobilisation on social media 130–133; organising grassroots campaigns for online manipulation 126–130; targeting opposition as internal enemies 133–135
social constructivism 73
social media 86–87, 100–101; architecture 68–70; authoritarian context 87–88; censorship of dissent on 213–214; conspiracy theories 92–100; emotive political mobilisation on 130–133; five filters in social media era 117–120; history and cultural background 92; removal requests 144–145; Shebab influencers 248–250; social media affordances 88–92
solidarity 146–148
Somali government 246–248
sourcing 118
spatial nationalism 56–57
state actors 107–108, 237–242, 251–252; adapting 112–115; background 108–109; digital jihad 250–251; filters in social media era 117–120; global landscape 243–244; learning 110–112; and non-state actors 242–243, 244–246; normalising 115–116; political economy of SDIOs 116–117; SDIO in Thailand 109–110; Shabab social media influencers 248–250; Shabab and Somali government 246–248
state-aligned media 142
state-aligned/state-linked troll armies 145–146, 214–215
state-sponsored disinformation 177–179, 188–189; Big Lie in Iranian regime's propaganda 181–1182; Big Lies in modern politics 179–181; celebrities 181–186; methodology 182–183; prominent dissidents in diaspora 186–188; protests of 2022 183–184
strategic deployment of conspiracy theories 97–100
strategic digital information operations (SDIOs) 1–6, 141–142, 209–211, 226–227; case studies 146–153; co-hashtagging as user practice 80–81; comprehensive understanding of 278–286; and cult tactics 257–259; digital manipulation

145–146; emotional and identity-based mobilisation strategies 146; future directions 286–289; goals 6–8; government control and censorship legislation 142–144; India 218–226; internet shutdowns and social media removal requests 144–145; propaganda campaigns via state-aligned media 142; SDIO realisation; Thailand 107–120; threatened democratic discourse 153–155; Turkey 213–218
strategic manipulation of digital media 50–53
strategy of information operations 254–256, 269–272; *The Alex Jones Show* 260–263; *The Ben Shapiro Show* 267–269; cult tactics and SDIOs 257–259; digital dissemination 257; methodological framework for analyzing masculinity in podcasts 259–260; online influence operations 256–257; *Tate Speech* 263–267
surveillance, diaspora 215–216, 221–223

targeting opposition 133–135
Tate Speech 20, 255, 259–260, 263–266, *264–265*, 270, 285–286
technosocial networked environments 70–72
Thailand 107–108; adapting 112–115; background 108–109; filters in social media era 117–120; learning 110–112; normalising 115–116; political economy of SDIOs 116–117; SDIO in 109–110
thought control 262–263, 266, 268
topics 32–33, *33*
trading up the chain 77, 80
transnational dynamics 10, 17–19, 283–284
transnationalisation 209–211, 226–227; India's SDIOs 218–219; India's transnational SDIOs 219–226; Turkey's transnational SDIOs 213–218
trolls, state-aligned/state-linked 145–146, 214–215
tropes, recurring 67–68
Turkey 124–126, 136–137, 209–213, 226–227; emotive political mobilisation on social media 130–133; organising grassroots campaigns for online manipulation 126–130; targeting opposition as internal enemies 133–135; transnational SDIOs 213–218
#TurkishCentury 131–132
Twitter *see* X (Twitter)

Ukraine 96–97
United Kingdom 29, 168, 193, 215, 217, 221–223
United States 3–6, 12–13, 57, 75–77, 90–97, 177–188, 193–195, 221–224, 241–242, 262, 283–284
user practice, co-hashtagging as 80–81
utilisation of digital tools 237–241, 251–252; digital jihad 250–251; global landscape 243–244; non-state actors 242–243, 244–246; Shabab social media influencers 248–250; Shabab and Somali government 246–248; state actors 241–242

violence 148–150
visibility politics 45–47, 57–58; conceptual consideration 47–48; digital media strategic manipulation and influence in elections 50–53; disinformation and misinformation 48–50; ethno-religious politics 53–55; spatial nationalism 56–57

warfare 278, 285–289
Western Balkan countries 193–195; disinformation and its conceptual anchoring 195–197; Russian disinformation campaigns 197–204
World Economic Forum (WEF) 77–78, 80, 196, 262

X (Twitter) 124–126, 136–137; emotive political mobilisation on social media 130–133; organising grassroots campaigns for online manipulation 126–130; targeting opposition as internal enemies 133–135