Digital (Dis)Information Operations
Fooling the Five Eyes

Edited by Melissa-Ellen Dowling

First published 2025

ISBN: 978-1-032-60179-3 (hbk)
ISBN: 978-1-032-60180-9 (pbk)
ISBN: 978-1-003-45794-7 (ebk)

Chapter 1

Decoding Digital (Dis)Information Operations

MELISSA-ELLEN DOWLING

DOI: 10.4324/9781003457947-2

The Open Access version of chapter 1 was funded by Flinders University.

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Introduction

1 Decoding Digital (Dis)Information Operations[1]

Melissa-Ellen Dowling

Introduction

States and societies are increasingly vulnerable to cyber-enabled information operations. From efforts to divide nations, undermine public policy, manipulate elections, and generate social discord, malign actors use the online realm to wreak havoc on our offline lives. In this book, we explore the digital disinformation dilemma that confronts liberal democracies, reflecting on shared socio-political challenges and solutions to contemporary information operations amongst the Five Eyes states and beyond.

Digitisation has reshaped how state and non-state actors manipulate adversaries' information environments. While the overarching objectives of information operations remain similar to pre-digital eras, digital technologies have enabled the tradecraft that malign entities deploy to become more sophisticated and less onerous. Within the last five years, we have seen, amongst many other incidents, digital attempts to interfere in elections through social media disinformation campaigns (Russia's Internet Research Agency), organised trolling of political opponents (India's Bharatiya Janata Party), hacked information communications technology (France's #MacronLeaks), and online political microtargeting (Cambridge Analytica).

While the causal consequences of attempts to undermine democratic processes through information operations often remain unclear, such operations, even if unsuccessful, can jeopardise the legitimacy of governments and governance, as well as erode democratic political culture (Dowling, 2022). Disinformation, trolling, hacking, conspiracy theories, and microtargeting (amongst many other types of information operations!) can all generate social fissures, leading to a less cohesive and more polarised society. Irrespective of their form or 'success', information operations distort the public sphere through inorganic information inputs that can make it more difficult to identify 'the truth' and engage in meaningful, constructive political debate. This is profoundly problematic given the importance of rich public debate for optimal policy and governance outcomes. Democracy depends on a healthy public sphere, and information operations infect and mutate the public sphere. Throughout this book, we identify the ways in which this occurs and offer insights into ways to safeguard against information operations in the digital era.

DOI: 10.4324/9781003457947-2

Of course, it would be remiss not to acknowledge that activities designed to distort information environments are not only a challenge for liberal democracies. Indeed, some of the most sophisticated and effective manipulation of public spheres is conducted by authoritarian governments on their own societies. Countries wherein freedom of the press, freedom of communication, and freedom of assembly are ill-protected (or non-existent) must also confront and contend with information operations, albeit in a distinct context wherein the state itself is the problem. However, this book focuses on the shared challenges experienced by liberal democratic states, that is, states wherein the public sphere should (theoretically) be open and 'free'. We contend that such states face comparable challenges, from similar types of adversaries, and have the potential to build on existing partnerships – particularly the Five Eyes intelligence alliance – to better protect their societies from digital information operations.

Why the Five Eyes?

While the challenges we discuss in this book confront many liberal democracies, we were particularly interested in exploring how information operations have unfolded and are being addressed in states that: (1) share strong social, political, cultural, and legal traditions; (2) already work together to tackle shared challenges through existing networks; and (3) demonstrate *prima facie* potential to deepen cooperation on the digital (dis)information dilemma. The Five Eyes – as a network of anglophone states with a history of cooperation on intelligence and security matters – presents a clear entry point for a discussion about strengthening international efforts with respect to information operations. The network (as Csorba details in Chapter 8 of this book, and Legrand enunciates in Chapter 9) is constituted by the US, the UK, Australia, New Zealand, and Canada, and has a legacy of sharing intelligence for the protection of democracy (Wells, 2020).

Aims of the Book

Part of the impetus for writing this book was to offer readers a 'one-stop shop' resource within which they could learn more about different social or 'human-centric' facets of information operations. Too often, we hear about information operations, disinformation campaigns, and cyber security from the confines of a narrow range of academic disciplines. Yet the topic can be explored through a variety of lenses. This book aims to generate a holistic human-centric perspective on the challenges of cyber-enabled information operations by bringing together diverse disciplinary perspectives from social science and humanities fields such as psychology, political science, law, sociology, international relations, security studies, and marketing. Together, these perspectives enable us to more effectively identify opportunities to address the challenge and increase the potential to enrich international collaborative efforts to safeguard liberal democracies from threats to their information environments.

We also observed that although scholars have engaged theoretically and empirically with cyber-enabled information warfare and operations in the last decade (see e.g. Blannin, 2021; Bolton, 2021; Lin & Kerr, 2019; Thrall & Mazanec, 2021; Ventre, 2016), few studies adopt interdisciplinary perspectives that tease out challenges for democratic institutions yet also identify opportunities for mitigation. Other publications that focus on facets of information operations such as disinformation (e.g. Hjorth & Adler-Nissen, 2019; Krafft & Donovan, 2020; McKay & Tenove, 2021; Shu et al., 2020), trolling, and microtargeting (e.g. Bodó et al., 2017; Dawson, 2021; Dowling, 2022), more effectively capture the scope of these challenges yet do so without firmly situating these activities within the broader cyber information challenge. Consequently, they do not, nor are they intended to, address the meta problem that our book focuses on: the socio-political threat that cyber-enabled information operations pose to the liberal democratic order. Although we maintain that although cyber-enabled information operations present a critical challenge to liberal democracies, together, the chapters of this book emphasise opportunities to mitigate the challenge through regulation, technological innovation, and international cooperation.

What Are Information Operations?

Our focus in this book is on cyber-enabled information operations though we chose to title the volume *Digital (Dis)Information Operations* to emphasise the extent to which disinformation permeates the information operations problem. The chapters in this book explore the range of mechanisms through which different actors use digital technology to manipulate information environments for political purposes. Sometimes, the term 'information warfare' is used synonymously with 'information operations' and 'influence operations'. In this book, we use the term 'information operations' to denote the broad spectrum of activities aimed at influencing an information environment for a political purpose, and 'information warfare' to refer to a narrower type of information operation that has more delineated military-strategic objectives wherein at least one party is a state or acting on behalf of a state (Ventre, 2016). Both are types of influence operations.

Actors: Who Conducts Information Operations?

For centuries, states have weaponised information for strategic and military advantage against adversaries, yet in today's digital world, they can do so with increased anonymity and greater reach. Digitisation has also empowered a host of non-state actors to engage in information operations. Non-governmental organisations, companies, terrorist groups, hacktivists, and other individuals can now partake in activities to influence information environments at scale (Denning, 2001). For example, ISIS regularly deployed propaganda to recruit, radicalise, and terrorise (Siegel & Tucker, 2018). Greenpeace has manipulated information environments as part of

a "strategic response" to climate change (MacKay & Munro, 2012), Cambridge Analytica engaged in psychological operations, data theft, and disinformation (Bakir, 2020), and the Syrian Electronic Army has hacked human rights' groups websites to advance its pro-regime agenda (Chapple & Seidl, 2021). Non-state actors that are sponsored by states to engage in offensive information operations are termed 'state-sponsored' and can serve as state proxies (Zannettou et al., 2020). For example, the Internet Research Agency conducted information operations against the United States on behalf of the Russian government (Mueller, 2019). As the chapters of this book demonstrate, the diversity of actors involved in information operations presents a host of challenges with respect to regulation, deterrence, and retaliation.

Aims: Why Are Information Operations Conducted?

The overarching objective of information operations is to achieve a political goal (Golovchenko et al., 2018), and many operations are intended to accomplish or maintain a strategic "competitive advantage" (Theohary, 2018, p. 1). Information operations can therefore be offensive, defensive, or both (Denning, 1999). They can be conducted to defend and protect one's own information environment or attack and manipulate an opponent's information environment. We explore both types of operations throughout this book.

Although the specific goals of each information operation differ, often, information operations are undertaken to:

- Influence public opinion (Arquilla & Ronfeldt, 2001; Terranova, 2007)
- Undermine an adversary's material capabilities (Blannin, 2021)
- Disrupt an adversary's communications infrastructure (Kopp, 2003)
- Protect one's own information infrastructure (Kopp, 2003)
- Support allies' decision-making (Dept. Defence, 2023; Morgan & Thompson, 2018).

As these goals indicate, information operations can be directed at hard and soft information targets. Soft targets are ideational and involve influencing populations, whereas hard targets are material and involve direct damage to and/or penetration of information systems. Some commentators refer to these as 'cognitive' and 'physical' domains of information operations (Condray & Romanych, 2005). Given our emphasis in this book on the social-cyber nexus, most of this book's chapters pertain to the cognitive domain. Yet, it is important to be cognisant of the range of information operations conducted.

Arenas: Where Are Information Operations Conducted?

Unsurprisingly, information operations are conducted in information environments. Such environments are multidimensional and dynamic, and these nuances

are captured in Robert Condray and Marc J. Romanych's (2005) definition of the information environment as follows:

> … a construct based upon the idea that the existence and proliferation of information and information systems creates a distinct operating dimension or environment. As a combination of tangible (physical information systems and networks) and intangible elements (information and decision-making), the information environment is both a resource for military operations and a medium in which armed forces operate.

As this definition highlights, information environments are constituted by a combination of tangible and intangible information elements. Cyber-enabled information operations are undertaken in digital information environments. Some environments that serve as sites of information operations are therefore ideational and are engaged with to exert cognitive influence (e.g. social media), whereas others (e.g. cyber infrastructure) are physical and are engaged in exerting physical damage.

Actions: How Are Information Operations Conducted in the Digital Era?

Since operations can be designed to exert cognitive and/or physical influence, we can, for analytical parsimony, consider two core types of information operation: social cyber-attacks and conventional cyber-attacks. However, some operations may engage in both forms of attack as part of the same strategic objective.

According to NATO (2020), social cyber-attacks involve "creating in people's minds a specific image of the world, consistent with the goals of the information warfare". Such attacks are used when information operations aim to influence public opinion and/or influence perceptions. 'Attacks' take place in the digital public sphere consisting of discussion boards, social media, and news media. Often, social cyber-attacks are conducted covertly using disinformation – "the deliberate creation and/or sharing of false information with the intention to deceive and mislead audiences" (Government Communication Service UK, 2021). Disinformation scholar Thomas Rid (2020) highlights the way in which disinformation is used to influence public perceptions. He explains how, "political passions are inflamed online in order to drive wedges into existing cracks in liberal democracies; perpetrators sow doubt and deny malicious activity in public, while covertly ramping it up behind the scenes" (Rid, 2020, p. 6). Of course, information can also be acquired or damaged via 'conventional' cyber-attacks. We use the term 'conventional' loosely here, given the rapid advances in technology which propel cyberwarfare beyond anything perhaps recognisable as conventional. Common techniques at the time of writing include malware, phishing, SQL injection attacks, cross-site scripting (XSS), denial of service (DoS), session hijacking, and credential reuse (Agrafiotis et al., 2018; Rapid7 2023).

The cyber attribution problem, wherein anonymity online often shields cyber attackers from being identified and held to account, complicates the role of law in mitigating cyber-attacks.

The Book's Structure

This book brings together insights from experts across diverse social science and humanities fields of research to provide a holistic human-centric perspective on the socio-political challenges of cyber-enabled information operations and opportunities for overcoming those challenges. The book is organised into three parts: (1) human techniques of digital (dis)information operations; (2) approaches to countering digital (dis)information operations; and (3) transgovernmental and intergovernmental initiatives and imperatives.

In the introduction, we explore the concept of cyber-enabled information operations and introduce the types of threats that constitute the digital (dis)information operations challenge plaguing liberal democracies today (Dowling).

The chapters of Part I ('Human Techniques of Digital (Dis)Information Operations') build on this foundation by investigating different human-centric techniques of information operations, such as the role of storytelling as a method to influence and persuade (Booth), the psychological predictors of susceptibility to conspiracy beliefs (Biddlestone et al.), and the use of psychographic profiling in elections (Farina et al.).

In Part II ('Human Approaches to Countering Digital (Dis)Information Operations'), the chapters consider ways to counter some of the techniques and effects of information operations by exploring regulatory measures to mitigate microtargeting (Dowling), education initiatives (Saletta), and approaches adopted outside of the Five Eyes context (Fallorina et al).

Part III ('Transgovernmental and Intergovernmental Initiatives and Imperatives') then offers insights into international and transnational possibilities for addressing the problems of information operations. The authors consider how the Five Eyes network may serve a protective function in its capacity to reinforce state sovereignty of participant states (Csorba), the ways in which policy networks are evolving with respect to the transforming information environment through AUKUS (Legrand), and the prospects for aligning law across international jurisdictions to combat fake news (Ray et al.).

We conclude with a reflection on the lessons the chapters provide on how to counter information operations beyond borders using predominantly social science approaches (Dowling). We contend that despite defying national borders, digital (dis)information operations are not insurmountable and can be addressed effectively through a constellation of national, transnational, and international responses.

Note

1 Aspects of this chapter were developed as part of a report prepared for the Australian Department of Defence: de Zwart, M., Henderson, S., Dowling, M. E., Lisk, J., & Lush, E. (2024). *Understanding the Law Applicable to Information Warfare.* https://hdl.handle.net/2440/140623.

References

Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation. <https://www.rand.org/pubs/monograph_reports/MR1382.html>

Bakir, V. (2020). Psychological operations in digital political campaigns: Assessing Cambridge Analytica's psychographic profiling and targeting. *Frontiers in Communication*, *5*. https://doi.org/10.3389/fcomm.2020.00067

Blannin, P. (2021). Modelling information warfare. *Journal of Information Warfare*, *20*(3), 90–107.

Bodó, B., Helberger, N., & de Vreese, C.H. (2017). Political micro-targeting: A Manchurian candidate or just a dark horse? *Internet Policy Review*, *6*(4), 1–13. https://doi.org/10.14763/2017.4.776

Chapple, M., & Seidl, D. (2021). *Cyberwarfare: Information operations in a connected world*. Jones & Bartlett Learning.

Condray, R., & Romanych, M. (2005). Mapping the Information Environment. *IO Sphere: Joint Information Operations Center*. Available at:https://www.hqmc.marines.mil/Portals/147/Docs/MCIOC/IORecruiting/MappingtheInformationEnvironmentIOSphere-Summer2005.pdf

Dawson, J. (2021). Microtargeting as information warfare. *The Cyber Defense Review*, *6*(1), 63–80. https://www.jstor.org/stable/26994113

Denning, D. (1999). *Information warfare and security*. Addison-Wesley.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In Arquilla & Ronfeldt (eds.) *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation. https://www.rand.org/pubs/monograph_reports/MR1382.html

Dowling, M. E. (2022). Cyber information operations: Cambridge Analytica's challenge to democratic legitimacy. *Journal of Cyber Policy*, *7*(2), 230–248. https://doi.org/10.1080/23738871.2022.2081089

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *International Affairs*, *94*(5), 975–994. https://doi.org/10.1093/ia/iiy148

Government Communication Service UK. (2021). *RESIST 2: Counter-Disinformation Toolkit*. https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf

Kopp, C. (2003). Shannon, hypergames and information warfare. *Journal of Information Warfare*, *2*(2), 108–118.

Krafft, P. M., & Donovan, J. (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

MacKay, B., & Munro, I. (2012). Information warfare and new organizational landscapes: An inquiry into the ExxonMobil–Greenpeace dispute over climate change. *Organization Studies*, *33*(11), 58-59. https://doi.org/10.1177/0170840612463318

McKay, S., & Tenove, C. (2021). Disinformation as a threat to deliberative democracy. *Political Research Quarterly*, *74*(3), 703–717. https://doi.org/10.1177/1065912920938143

Mueller, R. S. (2019). *The Mueller report*. Pandora's Box.

NATO 2020, (Dis)information Security, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Profile.

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., & Liu, H. (2020). Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(6), http://dx.doi.org/10.1002/widm.1385

Siegel, A. A., & Tucker, J. A. (2018). The Islamic State's information warfare: Measuring the success of ISIS's online strategy. *Journal of Language and Politics*, *17*(2), 258–280. https://doi.org/10.1075/jlp.17005.sie

Terranova, T. (2007). Futurepublic: On information warfare, bio-racism and hegemony as noopolitics. *Theory, Culture & Society*, *24*(3), 125–145. https://doi.org/10.1177/0263276407075960

Theohary, C. A. (2018). Information warfare: Issues for congress. *Congressional Research Service*. https://sgp.fas.org/crs/natsec/R45142.pdf

Ventre, D. (2016). *Information warfare*. John Wiley & Sons.

Wells, A. (2020). *Between five eyes: 50 years of intelligence sharing*. Havertown.

Zannettou, S., Caulfield, T., Bradlyn, B., De Cristofaro, E., Stringhini, G., & Blackburn, J. (2020, May). Characterizing the use of images in state-sponsored information warfare operations by Russian trolls on twitter. In *Proceedings of the International AAAI Conference on Web and Social Media*. 14, 774–785. https://doi.org/10.48550/arXiv.1901.05997