The Strategic Logic Of Digital Disinformation: Offence, Defence And Deterrence In Information Warfare

Chapter · October 2023

DOI: 10.4324/9781003190363-17

CITATION
1

READS
66

2 authors, including:

Hamid Akın Ünver
Özyeğin University
70 PUBLICATIONS **462** CITATIONS

SEE PROFILE

Routledge Handbook of Disinformation and National Security; edited by Rubén Arcos, Irena Chiru and Cristina Ivan
Format: 246_x_174_mm_(6.85_x_9.69) (174 × 246 mm); Style: Handbook_1; Font: Bembo;
Dir: Y:/2-Pagination/RHDN_RAPS/ApplicationFiles/9781032040509_text.3d;

14

THE STRATEGIC LOGIC OF DIGITAL DISINFORMATION

OFFENCE, DEFENCE AND DETERRENCE IN INFORMATION WARFARE

H. Akin Unver and Arhan S. Ertan

Introduction

Governments, state agencies and foreign policy institutions are increasingly deploying organised disinformation to distract and confuse their adversaries. In their 2020 report, Oxford Computational Propaganda Project identified organised, state-sponsored disinformation campaigns in 81 countries with a rapidly increasing number of "cyber troops" (semi-officially employed individuals working on state-sponsored information operations) and campaign intensities.[1]

While disinformation has largely been constructed as a form of "attack" perpetrated by authoritarian countries against liberal democracies, more democratic countries too, have engaged in organised disinformation attempts abroad. For example, both France and Russia engaged in disinformation campaigns in Mali, Central African Republic and other Sahel region countries to build influence and discredit opponents.[2] US State Department had a long-running program of digital disinformation against Jihadi content online, inserting its analysts into extremist discussions via pseudonyms and sharing false information to misdirect the militant group's online efforts.[3] In Hungary, the government used disinformation against Romania in order to make the case internationally that the refugee crisis was Bucharest's fault. Similarly, both Belarus and Poland instrumentalized disinformation during the most recent Ukrainian refugee crisis.[4] A 2021 European Parliament report has indicated that disinformation between nations has become rampant in Western Balkans, disrupting the political stability of the region and generating significant discrediting momentum for the EU.[5] From Brazil, Argentina to South Africa, India and Australia, a broad range of countries and regime types have been involved in organised disinformation.[6]

Propaganda, manipulation and misdirection have been long-standing tactics of diplomacy and international competition. In the last decade, and especially around the 2016 US Presidential election, "fake news" and disinformation became buzzwords of sorts that led to a rediscovery of the role of information in political competition. The biggest difference between the traditional and more recent debates on the matter is the digitalisation of information warfare and the subsequent scale, volume and speed advantages brought by this

 DOI: 10.4324/9781003190363-17

digitalization. The advent of Information and Communications Technologies (ICTs) brought about a faster information exchange medium where traditional gatekeepers like editors, censors or curators are of secondary importance and often irrelevant. While in more traditional media forms, broadcast is dependent on the approval of an intermediary individual or a group, with ICTs and social media, this approval is often hard to enforce with the sheer scale of information poured into such media venues. Although automated content moderation works in most cases, it can easily be circumvented.[7] With information gatekeepers out of the way, information becomes disintermediated (reduction in the use of intermediaries), with information suppliers (citizen journalists or anyone with access to social media) directly able to reach information consumers around the world, in real time.[8] The disintermediated nature of modern information exchange has rendered ICTs a conducive ground for misinformation (unintended spread of false information), disinformation (purposeful creation and dissemination of false information) and malinformation (deliberate use of accurate or inaccurate information with the purpose of harming an individual or people).[9]

To that end, the study of disinformation in the digital domain requires renewed attention as traditional studies of propaganda fail to address the speed, scale and the disintermediated nature of information sharing. Digital disinformation has been relatively-well studied in domestic political context, especially in the United States. However, opportunities for disinformation research within comparative politics and international relations (IR) fields are still very much untapped. Particularly, there is still no consensus in the field over how to conceptualise disinformation within the confines of IR: is it best understood as a "weapon", a "tactic", or is it simply a more robust form of propaganda?[10] How is digital disinformation different from disinformation in older media systems and how much does disintermediation affect the way people communicate and consume information, and as a result seek to alter or contribute to international affairs?[11] More importantly, why do countries choose to engage in disinformation against other countries and does disinformation as a foreign policy tool serve a different purpose than disinformation as a domestic political tool?

This chapter seeks to contribute to this emerging debate by exploring disinformation in international relations as a rational actor problem. It situates information warfare as a dyadic-dynamic interaction between the side that initiates disinformation (Attacker), the side that seeks to counter these efforts (Defender) and the international audience (IA) that affects the "winner" of this interaction. Ultimately, the chapter explores the payoff calculus of the Attacker and the Defender and aims to provide a path of exploration into the inner workings of deterrence in information warfare.

Why Do Countries Resort to Organised Manipulation? Unpacking the Demobilizing Logic of Disinformation

What accounts for the rapid explosion of digital disinformation in modern politics in the last decade? Although organised manipulation and propaganda have long been key tactics in statecraft and international politics, we do not yet have robust explanations for how mass digitalisation of communication changed its main parameters in inter-state political communication. Traditional works on propaganda treats political manipulation as a small part of a diverse array of communicative strategies, aimed to promote a political point of view, often through misleading and biased narratives.[12] However, such traditional works do not address the role of disinformation in political communication and how such disintermediation—coupled with vast size and lightning speed of ICTs—affects organised disinformation. A rapidly emerging, yet nascent body of work focuses overwhelmingly on the domestic