MP-IDSA Monograph Series
No. 85 April 2024

Influence Operations

The Sharp Power of Non-Kinetic Subversion

Adil Rasheed

MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA Monograph Series
No. 85 April 2024

Influence Operations: The Sharp Power of Non-Kinetic Subversion

Adil Rasheed

MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर परिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

ISBN: 978-81-965080-4-3

Disclaimer: The views expressed in this Monograph are those of the author and do not necessarily reflect those of the Institute or the Government of India.

First Published: April 2024

Price: Rs. 250/-

Published by: Manohar Parrikar Institute for Defence Studies and Analyses
No.1, Development Enclave, Rao Tula Ram Marg, Delhi Cantt., New Delhi - 110 010
Tel. (91-11) 2671-7983
Fax.(91-11) 2615 4191
Website: http://www.idsa.in

Layout & Cover by: Geeta Kumari & Virender Singh Rawat

Printed at: Pentagon Press LLP
206, Peacock Lane, Shahpur Jat
New Delhi-110049
Tel. (91-11) 26491568, 26490600
Fax: (91-11) 26490600
email: rajan@pentagonpress.in
website: http://www.pentagonpress.in

Contents

Preface

With an increase in protracted conflicts and attrition wars across global theatres such as in Russia-Ukraine and Arab-Israel regions, the importance of subversion using non-kinetic sharp power in the form of Influence Operations (IOs) has developed into a new cost-effective and often non-attributable form of hybrid warfare.

Having a lot in common with political warfare, psychological warfare and information operations of yore, this domain of intelligence has been revolutionised by 21st century Information Communication Technology (ICT) and has become an indispensable tool for shaping geopolitical outcomes without resorting to the use of direct military force. Thus, Influence Operations refer to the use of non-military means of psychological, technological, economic and political influence and subversion to undermine the security and governance of a targeted country.

Often succinctly defined as the organised attempt to achieve a specific effect among a target audience, Influence Operations are carried out by myriad actors today – from governments, politicians, non-State actors, special interest groups, foreign intelligence agencies and agents, etc. –promoting a range of ideological causes and disruptive agenda. The reason the impact of IOs has become highly problematic is because information can now reach a lot more people, much faster and further than ever before and it is very difficult to discern and prosecute foreign State and non-State 'malign influencers'.

The origins of Influence Operations can be traced back to the advent of psychological operations (PsyOps) during the World Wars, wherein propaganda, misinformation, and undue influence was used at an unprecedented level in scope and impact. In this regard, *Operation Mincemeat* and *Operation Fortitude* became highly popular, with Allied deception operations discomfiting German military intelligence on several occasions. However, by the time of the Cold War, the focus

had shifted from territorial acquisition to ideological supremacy between the capitalist and communist blocs. At that time, the CIA initiated a series of influence operations that targeted both domestic and international audiences. For instance, *Operation Chaos* was aimed primarily at monitoring anti-Vietnam War and Civil Rights activists, but it also sought to discredit such movements by associating them with foreign communist elements. On the other side, Soviet Union indulged in some of the most notorious subversive actions associated with "Active Measures".

However, it was with the coming of the Internet in the late 20th century that psychological operations underwent a major change. The Internet offered instant and extensive spread of information, making it exponentially easier to reach a global audience. Influence Operations could now be conducted in real-time, and reactions monitored instantly, allowing for rapid adjustments in strategy.

The Internet has today made it possible for even the non-State actors to engage in influence operations at a scale previously reserved for nation-states. Platforms like Facebook have become the new battlegrounds, with algorithms being constantly manipulated to amplify certain messages. The wide availability of smartphones has added another layer, turning individuals into potential nodes in a dynamic influence network.

The 2016 US Presidential election was a watershed in this regard, which illustrated the scale and impact that a well-executed Influence Operation could achieve, in that it exploited everything from social media campaigns to the hacking and leaking of sensitive emails.

Since then, social media platforms appear to have transformed into dangerous battlegrounds for influence operations. The widespread use of Facebook, X, Instagram, and LinkedIn offers a host of avenues for propagating narratives and for manipulating public opinion. Unlike traditional media channels, social media provides real-time feedback, which enables constant adjustments to the strategy.

In this monograph, the potential threat posed by 'foreign malign influence operations' has been studied at length, focusing on some of

the Influence Operation programmes of Russia, China, Pakistan, the US as well as non-State actors, like MNCs, NGOs and global terrorist organizations. Though exhaustive in scope, this monograph primarily seeks to introduce the subject of Influence Operations to the Indian readership, and does not claim to be an intensive study.

In one of its chapters, the monograph provides a glimpse of the various approaches and models used by countries for developing effective Influence Operations as part of their larger military campaigns. Today, there are several approaches, methodologies, and tools that assist countries in planning, executing, and in assessing Influence Operations.

The concluding chapter provides counter measures that a country like India can employ to protect itself from the malign impact of Influence Operations around the world, which have been broadly categorised under three heads: a) resilience building measures, b) deterrents and c) counter-measures.

As IOs are clandestine operations, few countries openly take credit for having conducted them and are largely discussed by countries that claim to be its victims (an exercise which in itself may be part of their IO disinformation against their adversaries). In any case, this study neither attributes nor denies any IO activity conducted by any country, non-State actor, agency or person, as discussed in it.

Chapter I

Introduction

Concept

In the 21st century, the war of ideas and seeding of thought patterns into the enemies' mind through the most persuasive mediums of technology has opened up the human cognitive frontier like never before. With the Information and Communications Technologies (ICT) revolution, information and psychological warfare is directed not just against enemy leadership or militaries, but against vulnerable communities and populations on a highly invasive and large scale, which has made sub-conventional and unconventional warfare far more complex and disruptive in their impact.

The hi-tech hybridization of political warfare, psychological warfare and information warfare has given rise to the concept of Influence Operations (IO), which is highly adaptive, low cost, insidiously sustainable and comes with added benefits of difficulty in attribution and prosecution under international legal frameworks. The efficacy of IOs to achieve highly damaging outcomes has thus become more evident in recent years.

A series of disrupted elections in the US and Europe, along with growing allegations of social media-aided uprisings and NGO-fomented revolutions has raised alarm over newer forms of 'sharp power' security threats posed to countries across the globe.

Influence Operations are thus the latest means for winning a war without physically waging it and meets Sun Tzu's idealized vision of victory:

> "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill"
>
> *The Art of War*[1]

---

[1] Sun Tzu translated and annotated by Lionel Giles, *The Art of War* by Sun Tzu, Special Edition, El Paso Norte Press, 2005, ISBN 0-9760726-9-6

As the recent Russia-Ukraine war has proven, conventional warfare has become a highly costly and unpredictable option for eliminating security threats. A more developed and lethal toolkit of Influence Operations (IO) today provides a varied and at-times custom built option, which is far more precise, practical and effective.

This study intends to provide a basic understanding of the term 'Influence Operations', showcasing the so-called 'toolkit' of its clandestine tactics and techniques, the use of IOs by non-state actors and case studies of four countries that are said to have developed their independent IO methods in this discipline.

The study merely charts the territory – even though there might be several aspects – techniques and issues left unexplored. For one, the monograph has not studied the institutional structures in various countries that develop IOs.

As a short theoretical study, it also does not have the scope to delve into specific Influence Operations conducted in detail as standalone case studies. Again, the focus of this chapter is on Influence Operations conducted by States and not by non-State actors — NGOs, terrorist groups, corporate organisations, etc.

In an attempt to study these issues in depth, this monograph is divided into sections. The first section is devoted to answering questions related to the meaning and definition of '*Influence'* and *'Influence Operations'* as well as provides a birds eye view of some of its salient operations. The section also studies some key cyber influence techniques that have revolutionized Influence Operations.

The second section pertains to the case studies of four countries which are said to have conducted Influence Operations against their enemies, namely China, Russia, the US, Pakistan and non-State actors in both the traditional offline and new online domains.

The concluding section recommends various approaches and models being used by countries for developing effective Influence Operations as well as ways for countries like India to counter or offset the impact of Influence Operations launched by a foreign State or non-State actor against it.

I - The Power of Influence

The Encyclopedia Britannica defines influence as "the power to affect, change or control somebody or something".[2] Surprisingly, Joseph S. Nye describes power in similar terms, "Power is the ability to affect others to obtain the outcomes you want."[3]

In International Relations, Joseph S. Nye believed that 'influence' is either seductive or coercive by nature. To elucidate his concept, Nye coined the term 'soft power' in the 1980s, which he said was the ability to "*co-opt* rather than *coerce"* and to this end believed "seduction" as a more potent form of influence. Thus, he wrote: "Seduction is always more effective than coercion, and many values like democracy, human rights, and individual opportunities are deeply seductive".

Nye's words proved prescient in that Western political concepts eventually triggered several so-called "colour revolutions" across the former communist bloc in Eastern Europe in the 1990s. However, Russia and China maintain that these revolutions were "externally fuelled acts" and the result of a new form of political and information warfare. But the charge of such insidious operations is also levelled by Western States against Russia and China, who have termed this modern form of cyber-fuelled political warfare as 'Influence Operations'.

Influence Operations (IOs) are said to have morphed the subtle instrument of Nye's 'soft power' into a malefic variant, called by Christopher Walker and Jessica Ludwig as "sharp power".[4] While democracies are said to employ public diplomacy to persuade foreign

---

2 Encyclopedia Britannica at https://www.britannica.com/dictionary/influence (last accessed online on 26 March 2024).

3 Geoffrey Cowan and Nicholas J. Cull (Eds.), *Public Diplomacy in a Changing World* (First Edition), The Annals of the American Academy of Political and Social Science Series, 616, April 2008, pp. 94-109.

4 Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence". *Foreign Affairs,* 16 November 2017.

governments and peoples with 'soft power', Christopher Walker states that "sharp power" comes more naturally to authoritarian regimes, as sharp power, "takes advantage of the asymmetry between free and unfree systems, allowing authoritarian regimes both to limit free expression and to distort political environments in democracies while simultaneously shielding their own domestic public spaces from democratic appeals coming from abroad."[5]

It is true that open and free sharing of reliable information, which is vital for the health of democracies, is today becoming increasingly susceptible to toxic disinformation and propaganda campaigns launched by authoritarian or military-run States, through both traditional and Internet-backed methods and techniques.

As Influence Operations using sharp power techniques are relatively low-cost and low-risk, with international regulations not providing adequate mechanisms to prosecute and punish foreign perpetrators of this form of warfare, the use of Influence Operations as a new constituent of 'hybrid warfare' has grown and is expected to develop rapidly in the future. As Information and Communication Technologies (ICT) advance rapidly, the battle to subvert public opinion in various countries is expected to rise. Another form of IO is religious radicalisation carried out by various State and non-State actors to undermine States and the international order.

Clearly, the advantages of the Internet in making high speed transactions, in developing clear strategies and tactics, and conducting low-cost flexible, agile, time efficient campaigns has revolutionized 21st century warfare, catapulting it to warfare in the "cognitive domain", now considered the sixth domain of warfare, after the five earlier domains of land, sea, air, space and information.

Influence Operations pertain not so much to the realm of information warfare or psychological warfare, but cognitive warfare, as they use

---

5 Christopher Walker, "What Is 'Sharp Power'?". *Journal of Democracy*, 29 (3), 2018, pp. 9–23.

dubious means to influence public opinion. As the ongoing Russia-Ukraine war demonstrates, conventional warfare is too costly and unpredictable, which makes non-conventional methods such as Influence Operations that much more attractive for they test, but rarely exceed, response thresholds. Skirmishes in the cyber, political, and cultural fields appear more preferable than kinetic skirmishes that often escalate into war with the risk of highly unfavourable outcomes.

II - Definitions and Scope of Influence Operations

Influence Operations refer to the targeting of any country's political institutions and processes — its public opinion, perceptions and even decision-making — through diplomatic, informational, psychological, intelligence, financial and other subversive means that are short of conventional warfare. Thus, Influence Operations appear to fall within the domain of both political warfare and information warfare.

As early as 2009, the RAND Corporation defined Influence Operations in its Report *as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviours, or decisions by foreign target audiences that further US interests and objectives."*[6]

Influence Operations offer the promise of victory through *"the use of non-military [non-kinetic], means to erode the adversary's willpower, confuse and constrain his decision-making, and undermine his public support, so that victory can be attained without a shot being fired".*[7]

---

[6] Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*, RAND Corporation, Santa Monica, CA, 2009 at https://www.rand.org/pubs/monographs/MG654.html. (last accessed online on 26 March 2024), Also available in print form.

[7] Anne Applebaum, Edward Lucas, "Wordplay and War Games", 19 June 2015 at http://www.cepa.org/content/ wordplay-and-war-games, (last accessed online on 26 March 2024).

Influence Operations can employ overt and permissible means of influence like public diplomacy and broadcasting, but the term is now being generally used in the context of covert and subversive operations linked to psychological warfare and propaganda, election meddling, crowd manipulation, infiltration into government bodies through corruption and support to underground resistance groups.[8]

According to Facebook, Influence Operations are *"coordinated efforts to manipulate or corrupt public debate for a strategic goal*."[9] With the Internet revolutionising the contemporary information environment, influence operations have been tremendously empowered in their scale, speed, and reach.[10] They seek to change not only what people think, but how they think and act and are part of 'cognitive warfare', where the collective human psyche itself becomes the battlefield.

However, Influence Operations are already making use of technological advancements not only in cyberspace, but also in artificial intelligence (AI), automation, and machine learning, combined with the growing availability of Big Data. With deepfake technologies rapidly advancing, it may soon become impossible to distinguish between real and falsified audio, video, or online personalities.

Assorted Toolbox of Influence Operations

One of the distinctions between information warfare and influence operations is that the former is employed during periods of war, whereas Influence Operations are conducted even when States may not be at war. Given this nature of Influence Operations, their toolkit

---

8 Danny Pronk, 'The Return of Political Warfare', *Strategic Monitor*, 2018-19 at https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019/the-return-of-political-warfare/ (last accessed online on 26 March 2024).

9 'Threat Report: The State of Influence Operations 2017-20', Facebook at https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf/, (last accessed online on 26 March 2024).

10 'Reconnaissance of Influence Operations', Lincoln Laboratory, Massachusetts Institute of Technology at https://www.ll.mit.edu/r-d/projects/reconnaissance-influence-operations, (last accessed online on 26 March 2024).

mainly constitutes non-military means of subversion and undue influence.

It is important to understand here the difference between coercion and undue influence. [11] The word 'coercion' refers to the use of physical force or threats to make someone do something against their will, while 'undue influence' refers to the use of persuasion or manipulation to gain an unfair advantage. Coercion is generally considered a criminal act, while undue influence is subtle and can be civil, social or political. While, coercion typically leaves the victim in an immediate state of fear and distress, undue influence may not be immediately recognized by the victim.

In fact, the toolkit of modern influence of operations employs both classical means of coercion and subversion employed by political warfare, information warfare and psychological warfare and cutting-edge technologies and innovations made in disinformation and subversion such as trolling, doxing and deepfake.

Public Diplomacy (Conventional and Subversive)

Public diplomacy refers to the effort of any government to communicate directly with the public of a foreign country, in order to win the support or acceptance of a foreign population for its policies or strategic objectives.

According to the Centre on Public Diplomacy at the University of Southern California, the term public diplomacy "has been widely seen as the *transparent* means by which a sovereign country communicates with publics in other countries aimed at informing and influencing audiences overseas for the purpose of promoting the national interest and advancing its foreign policy goals."[12]

---

[11] W. H. D. Winder, "Undue Influence and Coercion." *The Modern Law Review*, 3(2), 1939, pp. 97–120. *JSTOR* at http://www.jstor.org/stable/1089336 (Accessed 19 January 2024).

[12] 'Defining Public Diplomacy', USC Centre for Public Diplomacy, University of Southern California at https://uscpublicdiplomacy.org/page/what-is-pd (last accessed online on 26 March 2024).

It should be noted that the term was "coined in the mid-1960s by former US diplomat Edmund Gullion … partly to distance overseas governmental information activities from the term *propaganda*, which had acquired pejorative connotations".[13]

In this sense, public diplomacy includes such activities as

i. Events/Speeches of Leaders, Officials, Diplomats, Spokesmen, Experts

ii. Educational exchange programmes for scholars and students

iii. Diaspora interaction programmes

iv. Language training

v. Cultural events and exchanges

vi. Remote Conference Programmes on Business, Culture and Education

vii. Radio and television broadcasting

viii. Publication of promotional leaflets, magazines, booklets and brochures

ix. Establishment of Press Centres and Cultural Centres

x. Libraries and Information Resources

Such activities focus on improving the image or reputation as a way to shape the wider policy environment in the 'receiving' country.

In recent decades, the term has expanded in its scope and according to the so-called "new public diplomacy", it is not just sovereign States but even "a range of non-[S]tate actors with some standing in world politics – supranational organizations, sub-national actors, non-governmental organizations, and (in the view of some) even private companies – communicate and engage meaningfully with foreign

---

[13] Ibid.

population and thereby develop and promote public diplomacy policies and practices of their own."[14]

There are two kinds of public diplomacy. The first is branding or cultural communication. In this outreach to a foreign population, the government seeks to improve its image without seeking support for any particular or immediate policy or strategic objective. Branding may focus on highlighting three aspects: the promotion of the country's culture, its political values, and its foreign policies. The second type of public diplomacy involves public advocacy. Although branding focuses on making long-term cognitive changes in the perception of a foreign population, political advocacy seeks to build support within foreign population for immediate public objectives or to discredit that country's adversaries.

Public diplomacy efforts commonly entail the dissemination of strategic narratives in support of a State's "national culture, political ideals and policy".[15] These activities are widely accepted as legitimate means.

However, dubious 'sharp power' form of public diplomacy is being increasingly used by various countries these days. There is often a cacophony of charges made by rival States and blocs accusing the other with the dissemination of false, fake and deceptive strategic communication and narratives.

For instance, some of the techniques used in Influence Operations, not only provide false information to target populations about acts or policies of countries, but even information tainted with political biases and hidden agenda. In the name of public diplomacy, many States carry IO-tainted narratives to beguile and inveigle public opinion with the aim of causing internal strife within a country. Many foreign broadcasters airing their programmes in various States promote hate speech, seditious arguments or false debates. It may be directed at

---

[14] Ibid.

[15] Monroe E. Price, *Free Expression, Globalism, and the New Strategic Communication*, Cambridge University Press, Cambridge, 2014, p. 134.

justifying the repressive policies of a country through deceptive reasoning, misinformation and disinformation techniques.

Language-based educational programmes are exploited for political purposes as a means to spread a country's political ideologies and policies, to turn teachers or students into spies of the foreign government, to purposely develop long-term relations with influential members of the public for subversive purposes.

Mobilization of Diasporas for Political Purposes

A diaspora is a transnational community, which defines itself as a distinctive ethnic entity based upon its shared identity. Diasporas are formed either by a forced or induced historical migration from an original homeland to a host foreign country.

For Influence Operations, the politics of the diaspora is often studied in terms of its role in adversely influencing the politics and undermining the security interests of the host country.

However, it is also possible that certain sections of the diaspora may be used by either a host State, or operatives of a third country in the host State (like Pakistani intelligence encouraging Khalistan supporters in Canada), to launch seditious activities in the home country (like India) by involving certain disruptive elements within the diaspora. It is also possible that the diaspora acts independently and launches political campaigns free of any influence of any individual State (be it their homeland, their host States or any other State).

Media for Influence (Mainstream and Social Media)

Influence Operations often spread across both mainstream and social media domains. Authoritarian States may invest heavily in creating dubious narratives and networks for disseminating fake news and misleading narratives in and outside their countries. Certain countries may have a public relations agency like Pakistan's Inter-Services Public Relations (ISPR), as a wing of the country's security and intelligence apparatus for this purpose. It may employ writers, authors, academicians, journalists, even film, theatre and television personalities, for carefully developing strategic messages unrelated to facts. Young graduates may be employed as trolls and students of media studies may be sent abroad

to settle there and then subtly carry out public relations and propaganda campaigns there. The influence of many these States extends over each step along the global information supply chain, targeting newspapers, journals, books, movies, television, radio, digital platforms, smartphones and even mobile games.

Modern authoritarian States not only exercise full control over their national media outlets (print, electronic and digital), but seek to extend their control over national language media outlets operating privately from abroad in an attempt to stop any criticism of their governments coming from abroad and to possibly change the content in line with government propaganda. Many countries like Russia, China and Pakistan invest heavily in spreading their messages on social media – even on those they have blocked in their own countries (like Twitter, Facebook, YouTube and Instagram). Some countries supporting radical groups use the Dark Web and social media channels like Telegram to spread disinformation.

Today's Influence Operations in the social media have become highly sophisticated and complex. Certain governments employ "trolls and astroturfing (to simulate spontaneous popular movements), numerous "internet commentators" (falsely labelled the "50 cent army") are paid to "guide" public opinion. The trolls are used to defend, attack, stir controversy, insult, or harass their targets. Another way to simulate authenticity is to have content published by third parties in exchange for money (content farms, purchase of messages, of influence over an account, of an account or a page, or recruitment of "influencers").[16] The field of Influence Operations thus shifts from the cyber domain to the cognitive one.

Political Warfare (Disruptive Agitations, Election Meddling)

The so-called "malign foreign influence[r]" today is also charged with exploiting loopholes in democratic legislation regarding campaign

---

[16] P. Charon and J.-B. Jeangène Vilmer, *Chinese Influence Operations: A Machiavellian Moment*, Report by the Institute for Strategic Research (IRSEM), Paris, Ministry for the Armed Forces, October 2021.

donations to political parties, interfering in the country's policy making through corrupt lobbying practices, polarising public opinion through social media on emotive issues to sow social discord, or stimulating protest movements through crowd manipulation techniques to effect change in government or regime.

Democracies depend on a reliable political process, funded by clean money and non-interference by foreign State or non-State entities in the internal affairs of the State. They depend on the open, transparent and free sharing of information and are particularly vulnerable to the menace of Influence Operations that spread fake news, disinformation and propaganda. In the words of Danny Pronk, "The whole edifice of democratic governance is based on the assumption of an informed citizenry with a common sense of facts, shared public narratives and a solid trust in the information provided by institutions. This entire assemblage is threatened by carefully crafted [I]nfluence [O]perations and will only grow worse as new 'deepfake' technologies come into play."[17]

Some authoritarian States like China allege that Western powers have somehow mastered the art of stirring anti-regime protests in non-democratic countries around the world. They allege that non-government organisations (NGOs), under the control of Western intelligence agencies, carry out long-term infiltration in targeted countries.

Western agencies also support radical youth organizations and groom young leaders as their agents. In the name of providing aid, they also fund opposition parties and by radicalising and training protestors with literature like Gene Sharp's *From Dictatorship to Democracy,* stir so-called colour revolutions to overthrow targeted regimes.[18] Facebook and

---

[17] Danny Pronk, 'The Return of Political Warfare', *Strategic Monitor*, 2018-19 at https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019/the-return-of-political-warfare/ (last accessed online on 24 March 2024).

[18] 'GT Investigates: US Wages Global Color Revolutions to Topple Govts for the Sake of American Control', *Global Times*, 02 December 2021 at https://www.globaltimes.cn/page/202112/1240540.shtml last accessed online on 24 March 2024).

Twitter were used to organize protests, spread information, and communicate with the external forces. However, the veracity of these claims remains in doubt.

Economic Warfare (Market Disruption, Industrial Espionage)

Economic warfare refers to a belligerent country weakening the economy of a targeted State in order to damage that country's ability to fight a war or even function as a State effectively. Conventional means of economic warfare included ravaging the crops or destroying the economic infrastructure of a country. Other measures include imposing economic blockades, blacklisting, preclusive purchasing, cutting economic supply lines, etc.[19]

In the modern age, sanctions, tariff discrimination, the suspension of aid, freezing of capital assets, prohibitions on investments and other capitals flows and expropriation are common.

While these actions arguably come within the domain of hard power, Influence Operations in the economic sphere would include disinformation campaigns on trading leading to disruptions and volatility in stock markets, as well as currency markets,[20] which are vital for any country's economic interests.[21]

---

[19] Robert Luke Deakin, "Economic Information Warfare: Analysis of the Relation between Protection of Financial Information Infrastructure and Australia's National Security" , QUT Public University, Brisbane, https://eprints.qut.edu.au/15900/1/Robert_Deakin_Thesis.pdf (last accessed online on 24 March 2024).

[20] Jonathan E. Sanford, Currency Manipulation: The IMF and WTO," Congressional Research Service, CRS Report for Congress, RS22658, (28 January 2011), p. 3 at https://sgp.fas.org/crs/misc/RS22658.pdf. (last accessed online on 24 March 2024).

[21] Cathy L. Jabara, "How Do Exchange Rates Affect Import Prices? Recent Economic Literature and Data Analysis," US International Trade Commission, Office of Industries Working Paper No. ID-21 (May 2009), p. 4 at https://www.usitc.gov/publications/332/ID-21.pdf.((last accessed online on 24 March 2024).

Social media platforms are used by states and non-state actors to not only influence public opinion in targeted countries today, but they are also seen as having a negative effect on financial markets.[22]

In addition, through their sharp power influence and intelligence penetration, some States, are today accused of operating an elaborate system to spot foreign technologies, acquire them by all conceivable means, and convert them into weapons and competitive goods,without compensating the owners.

The Director of the US National Security Agency has called it "the greatest transfer of wealth in history."[23]

Culture and Education (Warfare in Cognitive Domain)

To overcome cultural domination of Western liberal culture — ranging from the media to movies, television shows, radio programmes, poetry, dance, literature, painting and even video games – many authoritarian States have started producing and promoting their own culture, which in itself may not be objectionable.

However, as such cultural propagation is often financed and produced by the State machinery itself, there is an understated strain of political messaging that works at the cognitive level to purposely influence – even misinform – foreign public opinion about the activities of the State.

Many cultural and language exchange programmes, like China's Confucius Institutes are supposedly not just language and cultural exchange programmes, but have allegedly become vehicles to project

---

[22] https://thestrategybridge.org/the-bridge/2021/11/3/bulls-bears-and-trolls-social-media-influence-operations-and-financial-market-risk (last accessed online on 24 March 2024).

[23] William C. Hannas, James Mulvenon and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* London and New York, 2013.

the "national power" of certain States and work as "propaganda outlets".[24]

It has also been alleged that some "oil and gas-rich" States of the GCC, like Qatar, are waging Influence Operations across the US educational system.[25] Some States also force their students studying abroad to acquire knowledge and technology still being developed by host countries through legal as well as illegal and covert means, like theft and espionage. Therefore, culture and education-related soft-power programmes are now used for sharp power Influence Operations.

Many States also establish links with think tanks of foreign countries, if not try to establish their own research centres in those countries. Their aim is to promote through the think tanks, insidious narratives or links with officials and leaders of strategic importance.

Cyber Influence Operations (CIOs)

Cyber Influence Operations (CIOs) deserve a special and more detailed understanding as they have revolutionized not only how information is produced, disseminated and consumed in Influence Operations, but even the way people and communities interact, forge relationships and can be mobilised.[26]

The ease of accessibility and low cost of entry that cyber technologies allow all kinds of States and non-State actors to engage in Influence

---

[24] Jerry Stepman, 'Confucius Institutes Closing, but Chinese Influence Operations Continue on College Campuses', *The Daily Signal,* 21 June 2022 at https://www.dailysignal.com/2022/06/21/confucius-institutes-closing-but-chinese-influence-operations-continue-on-college-campuses/ (last accessed online on 24 March 2024).

[25] 'Qatar is 'waging influence operations' across US education system: Legal organization', *Al Arabia News,* 15 May 2020 at https://english.alarabiya.net/News/gulf/2020/05/15/Qatar-is-waging-influence-operations-across-US-education-system-Legal-organization, (last accessed online on 24 March 2024).

[26] M. Bonfanti, 'An Intelligence-based approach to countering social media influence operations'*Romanian Intelligence Studies Review*, National Intelligence Academy, Bucharest, 2019.

Operations. There are a plethora of platforms, vectors, tools, and software easily available on the Internet and the Dark Web, which are easily and very cheaply available. Mechanisms to prosecute perpetrators of CIOs, even if identified, are virtually non-existent, especially if these operations are conducted online from foreign countries.

Social Media Replacing Mainstream Media (Deep Fakes): A huge market exists a huge market for bots and botnets as well as a range of forums, threads and chats (e.g. on discord, 4chan, Reddit, etc.), in which communities exchange information and support each other in using these tools and techniques.[27] Moreover, minimal knowledge is required to engage in basic CIOs, as only an elementary understanding of Photoshop and social media is needed to form and disseminate any photo montage. The meme maker (e.g. Imgflip) or fake tweet generators (e.g. simitator) can be easily availed. More sophisticated tools for making deep fake videos and photographs are also accessible and are getting user-friendly. FakeApp, for example, makes extremely realistic face-swapping videos.[28]

In the words of Daniel *Cohen* and Ofir *Bar'el*, "the internet has shifted the traditional model of information dissemination via the media and government entities to the dispersal of information by individuals and small groups, who (at times) operate without a clear hierarchical model, and are mostly lacking rules, regulations and government enforcement."[29] Therefore, conventional mainstream media has lost its monopoly on information dissemination, as many contending narratives and misinformation is being generated from online social media platforms.[30] Along with the agents of disinformation, other

---

[27] M. Baezner, P. Robin, *Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict,* Version 2. Center for Security Studies, Zürich, 2018.

[28] R. Chesney, D.K. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *SSRN Electronic Journal*, 2018.

[29] D. Cohen, D., O. Bar'el, 'The Use of Cyberwarfare in Influence Operations,' Tel Aviv university, 2017.

[30] B. Cronin, H. Crawford, 'Information Warfare: Its Application in Military and Civilian Contexts', *The Information Society*, 1999, pp. 257–263.

online miscreants such as hacktivists, cyber-terrorists, cyber criminals and lone hackers have vitiated the information landscape. This information highway has given a near free rein to all kinds of propaganda campaigns that Sean Cordey says is, "exploiting the illusory truth effect, in which repetition leads to familiarity and thus acceptance."[31]

Stealing of Psychographic Data:Artificial Intelligence (AI) technologies have greatly facilitated the collection, analysis and exploitation of psychographic data by States as well as private companies. Thus, AI has given States and non-State actors conducting CIOs increasing penetration, precision, and personalization of information targeting.

An embarrassing example of the threat occurred in 2010, when a British firm Cambridge Analytica, collected personal data of millions of Facebook users without their consent, which was then used by a "wide variety of actors (political and economic, foreign and domestic) to carry out in-depth electorate analyses and possibly also to target elections in a number of countries, including … Kenya, Malta, Mexico, the United Kingdom (i.e. the Brexit vote) and the United States (i.e. the 2014 midterms and 2016 presidential election)."[32] According to Herbert Lin, and Jaclyn Kerr, the targeted activities spawning from this scandal relied on a number of algorithmic recommendation tools that feed information confirming or reinforcing existing cognitive biases.[33]

However, AI technologies may also have its benefits in that they are being used for the early detection of CIOs and for in-depth analyses of social networks used by such campaigns.

---

[31] Sean Cordey, 'Cyber Influence Operations: An Overview and Comparative Analysis', Centre for Security Studies, October 2019 at https://css.ethz.ch/en/services/digital-library/publications/publication.html/c4ec0cea-62d0-4d1d-aed2-5f6103d89f93 (last accessed online on 25 March 2024).

[32] Ibid.

[33] Herbert Lin, and Jaclyn Kerr, 'On Cyber-Enabled Information Warfare and Information Operations', Oxford Handbook of Cybersecurity, May 2019 at SSRN: https://ssrn.com/abstract=3015680 (last accessed online on 25 March 2024).

CeTIOs and CeSIOs: To better understand and have effective counter and protection measures, CIOs have been divided into the following two categories:

i) Cyber-enabled technical influence operations (CeTIOs)

ii) Cyber-enabled social influence operations (CeSIOs)

- Cyber-enabled technical influence operations (CeTIOs)

These refer to cyberattacks conducted by ICOs to gain "unauthorized access to networks and systems in order to destroy, change, steal or inject information with the intention of influencing attitudes, behaviours, or decisions of target audiences".[34]

A major instance of CeTIOs includes the US Senate Intelligence Committee finding that Russian President Vladimir Putin allegedly ordered the 2016 hacking of Democratic Party accounts and the release of emails intended to harm Hillary Clinton's campaign.[35] Other examples are the 2007 DDoS (Distributed Denial of Service) campaign against Estonia, the 2013 hack of Associated Press's Twitter account and the Sony Corporation's hacking and leaking of sensitive information.

Again, hacks using malware (e.g. Trojans, viruses, worms, or rootkits) are carried out with the aim of discrediting and shaming a country's security. For instance, Chinese espionage is charged with breaching the US Office of Personnel Management and stealing 21.5 million records in 2015. This incident caused a major embarrassment for the US

---

[34] N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.), 'Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations,' 8th International Conference on Cyber Conflict Cyber Power, 2016, © NATO CCD COE Publications, Tallinn.

[35] Mark Hosenball, 'Senate committee concludes Russia used Manafort, WikiLeaks to boost Trump in 2016', 18 August 2020 at https://www.reuters.com/article/us-usa-trump-russia-senate-idUSKCN25E1US (last accessed online on 25 March 2024).

authorities as they were seen as being incapable of protecting sensitive information on their population.

The more high-end attacks like the hack of the Ukrainian electrical grid in 2015 and the US-Israeli Stuxnet cyber-attack first discovered in 2010 that melted a fifth of Iranian nuclear centrifuges, cannot be put in the category of Influence Operations, but in the domain of hard power technology.

- Cyber-enabled Social Influence Operations (CeSIOs)

Cyber-enabled social Influence Operations (CeSIOs) do not deploy techniques to affect the physical layer of cyberspace, but employ the semantic layer (i.e., information content) through various techniques to instigate and amplify political, diplomatic, economic, and military pressures. They focus on the social and cognitive domains, which may derive their methods and techniques from traditional sources of disinformation and propaganda, but are now further enhanced in cyberspace.[36]

The meaning of the term "disinformation" has been highly contested, but H. Allcott and M. Gentzkow define it as, "news articles that are intentionally and verifiably false and could mislead readers".[37] Disinformation activities may employ advertising, satire, propaganda, misappropriation, manipulation and fabrication.

Following is the list of few techniques used for spreading disinformation through CeSIOs tools and techniques:

- *Socio-Cognitive Community Hacking*: This technique exploits the cognitive vulnerabilities, psychosocial trigger points and emotions (e.g., fear, anger, hate, anxiety, honour, etc.) of a community,

---

[36] P. Pamment, H. Nothhaft, H. Agardh-Twetman, A. Fjällhed, Book: *Countering Information Influence Activities: The State of the Art*, Lund University, Lund, 2018.

[37] H. Allcott and M. Gentzkow, "Social Media and Fake News in the 2016 Election", *Journal of Economic Perspective,* 2017, (Vol. 31, Issue 2) pp. 211 – 235.

group or person to influence their behaviour. Often the narratives here are not even fully developed, but just introduce a doubt or an emotive trigger to build a desired perception that may play on the vulnerabilities of the target audience. One of such practices is "swiftboating", whereby an electoral candidate faces allegations just before elections and does not get the time to respond.

Psychographic advertisements target a carefully identified vulnerable audience on various Internet platforms. For example, so-called *dark ads* were posted on Facebook during the 2016 US presidential election that were visible only to an intended audience and paid for by the Internet Research Agency (IRA), an organization with alleged links to the Russian government. US experts allege that over 3000 types of *dark ads* that focused on controversial topics (e.g., race, gay rights, gun control and immigration) were shown to selected audience to polarize the political debate and the electorate.[38]

Other techniques of social hacking employ certain disinformation techniques, such as exploiting *social proof, the bandwagon effect, and selective exposure*. The tendency of people to believe a statement not based on sound arguments but because many others believe in it is a technique called social proofing, which is used by CIOs in social media outlets to promote disinformation. This often relates to using the deceptive technique of *astroturfing*, i.e., "suggesting that there are a lot of people who support a political agenda, while in fact there is no such support".[39]

The technique of selective exposure often leads people to meet like-minded views on social media, a technique used to polarise

---

[38] R. DiResta, K. Shaffer, B. Ruppel, D. Sullivan, R. Matney, R. Fox, J. Albright B. Johnson, 'The Tactics & Tropes of the Internet Research Agency' (Article), New Knowledge, 2018.

[39] P. Pamment, H. Nothhaft, H. Agardh-Twetman, A. Fjällhed, *Countering Information Influence Activities: The State of the Art*, Lund University, Lund, 2018.

societies. Algorithms on social media platforms can enable forms of selective exposure by contributing to the creation of filter bubbles or echo chambers, with the former causing a state of intellectual isolation through algorithmic personalization while the latter describing "organically created internet sub-groups, often along ideological lines, where people only engage with others with whom they are already in agreement".[40] These techniques are directed at causing polarization in society, fragmentation of online opinion and political division.

- *Para-social hacking*: One-sided relationships of common people formed with celebrities, officials, intellectuals or even strangers on social media — like on Twitter, Instagram, or Snapchat — converts the former ardent followers of the latter and makes them vulnerable to the views and opinions of their role models, and at times the latter use them to promote their social and political agenda. These relationships can be exploited by foreign States if they closely associate with important celebrities or intellectuals inside a country, with a huge para-social following.

- *Forgeries, False Identities, Potemkin Village*: CIOs may resort to illicit propagation of false evidence on social media or the Dark Web with the aim of "cultivating distrust among citizens and inducing them to question the integrity, reliability and trustworthiness of the media" and public institutions. They may forge fake letterheads, official stamps and signatures, sometimes combined with the supposed leaking of forged communiqués to justify their disinformation campaign. Similarly deceptive identities can be grouped by mixing authentic and second-hand identities to disseminate falsehood on the Internet. Similarly, "potemkin villages of evidence" can be presented on social media through an array of illegitimate or fake research appearing in so-called journals or think-tank publications to present a false narrative as a product

---

[40] Jonathan Bright, 'Explaining the Emergence of Echo Chambers on Social Media: The Role of Ideology and Extremism', SSRN Electronic Journal, 2016, 10.2139/ssrn.2839728.

of careful scholarly consideration. These deceptions are directed at creating a Woozle effect, where one sees what one wants to see rather than what is actually there.

- *Misuse of Bots and Botnets:* A short form for robots, bots refer to "a piece of automated computer software that performs highly repetitive tasks along a set of algorithms".[41] A botnet is a portmanteau of the words "robot" and "network" and refers specifically to a group of Internet-connected devices that run one or more bots. Botnets can be used to perform Distributed Denial of Service attacks, steal data, send spam, and allow the attacker to access the device and its connection.

  In CIOs, four main social bots are in use: hackers, spammers, impersonators and sock puppets. According to Sean Cordey, "Hackers are employed in ICOs to attack websites or networks or help establish botnets used for DDoS attacks. Spammers are created to post content in forums or commentary sections (including malicious links for phishing) in order to help spread disinformation and other illegitimate content, or simply to crowd out legitimate content. Impersonators focus on replicating natural behaviour in order to best engage with political content on social media platforms or to scam people, while sock puppets are semi-automated lookalike or imposter accounts controlled and coordinated by individuals to conduct false-flag operations or to disseminate disinformation."[42]

- *Trolling, Flaming and Doxing*: 'Trolling' refers to the deliberate attempt by a user or social bot to annoy, trigger, aggravate disrupt, offend or cause trouble by posting provocative and

---

41 K. Michael, "Bots Trending Now: Disinformation and Calculated Manipulation of the Masses", Published in: IEEE Technology and Society Magazine (Volume: 36, Issue: 2, June 2017), pp. 6 – 1.

42 Sean Cordey, 'Cyber Influence Operations: An Overview and Comparative Analysis', Centre for Security Studies, October 2019 at https://css.ethz.ch/en/services/digital-library/publications/publication.html/c4ec0cea-62d0-4d1d-aed2-5f6103d89f93 (25 March 2024).

disruptive content on online social media platforms.[43] While *trolling* might be direct at a particular set of individuals or naïve users, 'flaming' is directed against a larger community or readers in general.[44]

Meanwhile, 'doxing' or 'doxxing' is the act of publicly providing personally identifiable information about an individual or a group on the Internet, usually with malicious intent. These techniques can be used to malign important political leaders, decision-makers or role models in a nation or community by CIOs to create social discord and disharmony. States or companies may employ highly organized trolls working in "troll factories" or there could be individual trolls. Trolling, doxxing and flaming are particularly effective when the intent is to polarize debates, silence diverse opinions, distract online debates or to disrupt the formation of public opinion.

- *Other Techniques:* Humour, satire and memes (funny pictures with jokes written on them) are not always used on the Internet just for the purpose of entertainment or relief, but at times to covertly manipulate and influence "hearts and minds" of the public towards a political agenda or goal. Other techniques include 'flooding' (to overload a platform with conflicting opinions to hamper credible assessment), 'cheerleading' (to bombard spurious narratives through various Internet channels to give it popularity and thereby legitimacy), 'raiding' (synchronised attacks to crowd out and silence diverse opinions on a political issue. and 'polarization' (a strategy to force the support for any of the two extremes on a specific issue and to weaken a moderate or centrist position). At times, spammer bots, trolls or DDoS attacks are used for effecting the above techniques.

---

[43] E. Moreau, "Internet Trolls and the Many Ways They Try to Ruin Your Day", *Lifewire*, at https://www.lifewire.com/ types-of-internet-trolls-3485894. (last accessed online on 25 March 2024).

[44] Susan Herring & Job-Sluder, Kirk & Scheckler, Rebecca & Barab, Sasha. (2002). Searching for Safety Online: Managing "Trolling" in a Feminist Forum. The Information Society. 18. 10.1080/01972240290108186, pp. 371– 84.

Chapter II

Russia's Influence Operations

Campaigns by Four Countries

This study looks into the research conducted by various States like Russia, China, the US and Pakistan on Influence Operations' approaches and methodologies, and proposes measures on how India should prepare itself to overcome such hybrid warfare.

Influence Operations: Russia

It is widely held in the West that the Russian Federation has sought to undermine the democratic processes and institutions in many countries in recent years, mainly in Europe and North America, through what they term is its "global malign influence operations and election influence activities".[45] Many of Russia's Western detractors present a long list of its alleged influence operations activities including control of the Press in foreign countries, forgery of documents, spreading of rumours and insinuations, reflexive control (feeding an opponent selected information to elicit the desired decision), lies and altered facts, interference in democratic elections of foreign countries, subversion and exploitation of a country's academic, political, economic and media figures, poisoning regime's opponents abroad,[46] cyber-attacks on vital

---

[45] Antony J. Blinken, 'Targeting Russia's Global Malign Influence Operations and Election Interference Activities', Press Statement, US Department of State, 29 July 2022 at https://www.state.gov/targeting-russias-global-malign-influence-operations-and-election-interference-activities/ (last accessed online on 25 March 2024).

[46] 'Russia's Means of Global Influence', RAND, National Security Research Division at https://www.rand.org/nsrd/projects/russian-arms-sales-and-sanctions-compliance.html (last accessed online on 25 March 2024).

infrastructure of foreign countries, and setting up State-sponsored media criminal and mafia networks abroad.[47]

Western governments and media hold Russia responsible for a whole range of influence operations conducted against them in the last decade-and-a-half. They cite the 2007 cyber-attack on Estonia that targeted that country's parliament, ministries, bank and media organizations,[48] the digital attack on the German parliament in 2015,[49] on the Lithuanian and Montenegro parliaments in 2016[50] and 2017[51], hacking against French presidential candidate Emmanuel Macron in 2017[52], and the digital penetration into the most infamous computer network of the Democratic National Committee during the 2016 US presidential elections.[53] Russian non-government organizations also hacked Western

---

47 David Salvo and Andrew Andell, 'The Active Measures Orchestra: An Examination of Russian Influence Operations Abroad', German Marshall Fund at https://www.gmfus.org/news/active-measures-orchestra-examination-russian-influence-operations-abroad(last accessed online on 25 March 2024).

48 Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', *The Guardian*, 17 May 2007 at https://www.theguardian.com/world/2007/may/17/topstories3.russia(last accessed online on 25 March 2024).

49 'Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag', *Netzpolitik*, 19 June 2015 at https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/(last accessed online on 25 March 2024).

50 'Lithuanian Parliament Under Cyber Attack', *Euractiv*, 12 April 2016 at https://www.euractiv.com/section/digital/news/lithuanian-parliament-under-cyber-attack/ (last accessed online on 25 March 2024.)

51 John Leyden, 'Kremlin Hackers' new Target: Montenegro', *The Register*, 6 June 2017 at https://www.theregister.com/2017/06/06/russian_hackers_target_montenegro/ (last accessed online on 25 March 2024).

52 Eric Auchard and Bate Felix, 'French candidate Macron claims massive hack as emails leaked', Reuters, 6 May 2017 AT https://www.reuters.com/article/us-france-election-macron-leaks/french-candidate-macron-claims-massive-hack-as-emails-leaked-iduskbn1812az (last accessed online on 25 March 2024).

53 'Russian Government Hackers Penetrated DNC', *Washington Post*, 14 June 2016 at https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-

media organizations such as France's TV 5 Monde and the World Anti-Doping Agency. [54,55]

Revival of Cold War 'Active Measures'

According to Western strategic experts, Russia has in recent years, revived its covert political operations, from alleged disinformation campaigns to fomenting insurrections, while incorporating new technologies and advanced forms of communication into its IO toolkit.

Russia had a developed tradition of conducting political warfare, dating back to the Soviet era, if not to tsarist Russia. From the 1950s, the Soviet Union used the term '*Aktivnye meropriyatiya* ("Active Measures") for its wide array of covert and deniable political influence and subversion operations involving the "establishment of front organizations, the backing of friendly political movements, the cultivation and protection of pro-Russian intellectuals, leaders and public figures abroad, the orchestration of domestic unrest and the spread of disinformation"[56]. To be fair though, similar tactics was often used by the British Special Operations Executive (SOE) and US Office of Strategic Services (OSS), during and after the Second World War.[57]

---

trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?hpid=hp_rhp-banner-main_dnc-hackers-1145a-banner%3Ahomepage%2Fstory&utm_term=.3d6c83451e98 (last accessed online on 25 March 2024).

54 Gordon Corera, 'How France's TV5 was almost destroyed by "Russian hackers",' BBC, 10 October 2016 at https://www.bbc.com/news/technology-37590375 (last accessed online on 25 March 2024).

55 David Salvo and Andrew Andell, 'The Active Measures Orchestra: An Examination of Russian Influence Operations Abroad', German Marshall Fund at https://www.gmfus.org/news/active-measures-orchestra-examination-russian-influence-operations-abroad (last accessed online on 25 March 2024).

56 Mark Geleotti, 'Active Measures: Russia's Covert Geopolitical Operations', Marshall Centre, June 2019 at https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0 (last accessed online on 25 March 2024).

57 Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West,* Penguin, 2000.

However, the covert "active measures" were scaled down and eventually ended during Gorbachev's reform era and following the dismemberment of the USSR. But the growing threat of NATO expansion into Eastern Europe and the increase in democratic "colour revolutions" in countries of the former communist bloc, are said to have renewed concerns among Russian decision makers, that their country still faced a constant and covert threat of subversion from outside.

In 1929, Joseph Stalin ordered the establishment of a Special Disinformation Office. Apart from developing and disseminating all kinds of propaganda, it soon started guiding various insurgencies around the world, and its agencies are said to have become "the primary instructors of guerrillas worldwide".[58] Thus after the Second World War, Soviet security organizations were often viewed as having played a key role in installing puppet communist governments in Eastern Europe, China, North Korea and even Afghanistan.

A former Soviet intelligence officer Stanislav Lunev said that Soviet intelligence agencies spent over a billion dollars in the late 1960s and 1970s to promote peace movements against the US war with Vietnam. Lunev even claimed that "the GRU (Russia's Main Intelligence Directorate) and the KGB helped to fund just about every anti-war movement and organization in America and abroad".[59]

Several Soviet "active measure" operations were exposed to the world by 'Mitrokhin Archives", which are a collection of handwritten notes and official documents which were smuggled by former Soviet official Vasili Mitrokhin for over 30 years when he served as a KGB archivist in the foreign intelligence service and as the first chief directorate. When he defected to the UK in 1992, he brought six full trunks of archives with him. Many of the "active measure" operations by the USSR against the United States, were exposed by the so-called Mitrokhin Archives.[60]

---

58 Viktor Suvorov, *Inside Soviet Military Intelligence*, Macmilllan, New York, 1984.

59 Stanislav Lunev, *Through the Eyes of the Enemy: The Autobiography of Stanislav Lunev,* Washington, D.C, Regnery Publishing, Inc., 1998.

60 Vasili Mitrokhin, Christopher Andrew, *The Mitrokhin Archive: The KGB in Europe and the West,* Penguin, 2000.

Some of the operations involved disseminating fabricated conspiracy theories, such as false claims that John F. Kennedy and Martin Luther King Jr. had been assassinated by the CIA, mailing bogus letters from the Ku Klux Klan and placing explosive packages in "the Negro section of New York" (Operation Pandora), to create racial tensions in the US, and fabricating the story that the AIDS virus was developed by US scientists at Fort Derrick.[61]

Even today, Western States allege that the current intelligence service, the Foreign Intelligence Service of the Russian Federation (popularly known as the SVR) seeks to undermine former Soviet satellite States in Eurasia. They blame Russia for infiltrating the political/military hierarchy of Western States by bribing, extorting, and even blackmailing vulnerable political figures to further its interests. Russian military intelligence, for example, is alleged to have instigated a 2016 plot to overthrow the pro-NATO government of Montenegro. Russian social media operations are said to have helped its special forces seize Crimea and its IO operations were found supporting separatists in the Donbass region. They are likely operating in several NATO-allied countries.

Information Confrontation: A Distinct Form of Hybrid Warfare and IO

In the post–Cold War era, Russia has developed a new kind of strategic thinking that promotes hybrid warfare, at an even higher level than in the 20th century. This approach is conceptualised under the term 'Information confrontation', or *informatsionnoe protivoborstvo* (IPb), which is different from Western conceptions about information in conflict. IPb is a multi-faceted strategy that covers all three domains related to information —physical, digital and cognitive.

In Western strategic thinking, information operations generally cover the domain of cyberspace and the physical infrastructure and devices that support or are enabled by it. However, Russian information warfare

---

[61] Mark Kramer, "Lessons from Operation "Denver," the KGB's Massive AIDS Disinformation Campaign", *The MIT Press Reader*, 26 May 2020.

(IPb) incorporates not just the physical and digital domains, but expands beyond them to include the domain of human cognition and emotion.[62]

According to Russian strategic thought, as Keir Giles puts it, "there is no distinction between information stored in a computer or in the human mind, just as there is no distinction between the way information is transferred between those storage spaces".[63]

The implication is that information conceptualized in terms of its various spaces, means of transmission, and broad scope is subject to use as a tool, target, or domain of information confrontation operations.

According to NATO's own admission: "There is still a lack of consensus when it comes to defining all the elements that make up the strategic application of power in the information domain. Regarding the use of terms like Information Warfare (IW), Psychological Operations (PsyOps), Influence Operations (IO), Strategic Communications (STRATCOM), Computer Network Operations (CNO), and Military Deception (MILDEC), there is a lot of confusion as there are numerous conflicting definitions, and these terms are used in different contexts to describe different objectives and actions."[64]

However, when it comes to Russia's conception, all the tools of the grey zone or hybrid warfare come under the gamut of "information confrontation". In the words of Russian experts S. G. Chekinov and S. A. Bogdanov: "Wars will be resolved by a skilful combination of military,

---

[62] Keir Giles, *Handbook of Russian Information Warfare*, "NDC Fellowship Monograph Series", Fellowship Monograph 9, NATO Defense College, 2016, p.6.

[63] Lesley Kucharski," "Russian Multi-Domain Strategy against NATO: information confrontation and US forward deployed nuclear weapons in Europe", Centre for Global Security Research, Lawrence Livermore National Laboratory, 2018.

[64] P. Brangetto and M. A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in N. Pissanidis *et. al.* (eds.), *8th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, June 2016 at https://ccdcoe.org/sites/default/files/ multimedia/pdf/CyCon_2016_book.pdf (Accessed 20 June 2016).

non-military, and special nonviolent measures that will be put through by a variety of forms and methods and a blend of political, economic, informational, technological, and environmental measures, primarily by taking advantage of information superiority. Information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources).”[65]

Thus, Giles states that in the Russian conceptual framework: “Information can be stored anywhere, and transmitted by any means – so information in print media, or on television, or in somebody’s head, is subject to the same targeting concepts as that held on an adversary’s computer or smartphone”.[66]

He adds that the transmission of this information can also be by any means and may even include introducing corrupted data into a computer across a network or from a flash drive. Such acts are conceptually no different from placing disinformation in a media outlet, or causing it to be repeated in public by a key influencer.

Russia’s Propaganda Method

US security experts allege that unlike Soviet times, Russia no longer aims to convert the world to a particular ideology and that its propaganda efforts are deployed to cause ideological confusion and strife rather than promoting any singular political ideology.

Russia’s present strategic objectives vary and information campaigns often advance more than one strategic or specific objective. Thus, it is said that these campaigns may seek to stoke internal differences between

---

[65] S. G. Chekinov and S. A. Bogdanov, “Ïðîãíîçèðîâàíèå õàðàêòåðà è ñîäåðæàíèÿ âîéí áóäóùåãî: ïðîáëåìû è ñóæäåíèÿ” (Forecasting the nature and content of wars of the future: problems and assessments), Voennaya Mysl’ (*Military Thought*), 10, 2015, p. 44-45.

[66] Keir Giles, no. 62, p.10.

different parties or sections of society within a country, or between two or more countries, malign the West, respond to accusations of wrongdoings, or glorify Russian policies or leaders.

In addition, there could be the use of fabrication, misappropriation, obfuscation, rhetorical fallacies, selective use of facts, emotive messaging, conspiracy theories etc. More important, these campaigns may not take any ideological sides but seek to foment and exacerbate differences within a State. Russia is said to carry out its information warfare using a variety of mediums —including television, newspapers, radio broadcasts, live events, online media and social media—which might promote the likelihood that audiences are exposed to certain messages, and exposure to or awareness of a message could increase its potential influence.

It is alleged that Russia effectively uses strategic communications which shapes political narratives against many countries for the international audience as well as for citizens of the targeted countries. Its media outlets such as *Russia Today* and *Sputnik News* are among the most well-known channels for carrying out this strategy, but the country is also accused of infiltrating and using television channels in other countries to spread its propaganda, of funding European think tanks to promote its views; of employing large numbers of Internet trolls, bots, and fake news farms, as part of its media influence operations.

A RAND report by Christopher Paul and Miriam Matthews states that Russian propaganda is produced in incredibly large volumes and is broadcast or otherwise distributed via a large number of channels.[67] According to them, "this propaganda includes text, video, audio, and still imagery propagated via the Internet, social media, satellite television, and traditional radio and television broadcasting." Western experts allege that the producers and disseminators of this Russian "propaganda" include a substantial force of paid Internet "trolls" who counter anti-

---

[67] Christopher Paul and Miriam Matthews, "The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, Santa Monica, CA, 2016 at https://www.rand.org/pubs/perspectives/PE198.html (last accessed online on 25 March 2024).

Russian themes through several online chat rooms, discussion forums, and comments sections on news and other websites."[68]

Social Media in Russia's Information Confrontation Arsenal

At the onset of the Ukraine crisis in 2014, Russian security experts had integrated social media platforms into its information confrontation arsenal. Russian military thinkers and experts viewed the rise of social media as a threat to Russia's security, but they also embraced it as a low-cost and highly effective offensive weapon.

The Russian military's embrace of social media is partly rooted in the perceived advantage of leveraging a relatively low-cost capability to undermine a superior opponent in conventional warfare, while insulating State-sponsored actors from direct attribution. Western security experts allege that Russia and its agents employ deceptive identities, social engineering, native advertising, and stealth marketing on social media to distribute their so-called "subversive information". They claim that personalization of social media communication by micro-targeting users and groups is employed in these operations.[69]

Charges of Russia's Intervention of 2016 US Presidential Elections

The US government has charged Russia with interfering in the 2016 presidential elections to undermine Democratic candidate Hillary Clinton's campaign and for promoting the candidacy of former

---

[68] See Adrian Chen, "The Agency," *New York Times Magazine*, 2 June 2015, and Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia and 'The Interpreter' newsletter, New York Times, 2014.

[69] Matthews, Miriam, Alyssa Demus, Elina Treyger, Marek N. Posard, Hilary Reininger, and Christopher Paul, *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe,* RAND Corporation, RR-3160-EUCOM, 2021, as of June 22, 2023 at https://www.rand.org/pubs/research_reports/RR3160.html

President Donald Trump. The US intelligence community believes Russian President Vladimir Putin directly ordered this operation, allegedly codenamed *Project Lakhta*.

According to the official Mueller Report,[70] although there were contacts between the Trump campaign and Russian officials but there was insufficient evidence to level charges of either conspiracy or coordination against President Trump or his associates.[71] However, the Report found The Internet Research Agency (IRA), based in St Petersburg (Russia) — which is described as a troll farm — had created thousands of social media accounts of purported Americans supporting extremist political factions and planned or promoted events in support of Donald Trump. The Report states that messages through these fake accounts reached millions of people using social media from 2013 to 2017.

According to the Report, Russian government-controlled media also spread fabricated articles, while computer hackers affiliated with the GRU are alleged to have infiltrated information systems of the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), as well as officials of Hillary Clinton's campaign; most notably chairman John Podesta. Stolen files and emails were publicly released through WikiLeaks, DC Leaks, Guccifer 2.0 and Wikileaks.

---

[70] Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, (2 Vols), 448 pp., at www.justice.gov/storage/report.pdf) (last accessed online on 25 March 2024), *The New York Review of Books*, 66 (9), 23 May 2019.

[71] Brian Ross, Rhonda Schwartz, James Gordon Meek, "Officials: Master Spy Vladimir Putin Now Directly Linked to US Hacking", , ABC News, 15 December 2016 (Accessed 15 December 2016).

Chapter III

Influence Operations: China

In the words of Kerry Gershaneck, the People's Republic of China (PRC) has managed to invert Clausewitz' famous dictum that "war is the extension of politics by other means" into "influence operations is an extension of war by other means".

Mao infamously equated influence with "xi-nao" (which means brainwashing), which has remained one of the principles on which the Chinese Communist Party (CCP) spreads and maintains its influence both within and outside its borders. In the 1990s, the CCP carefully cultivated an international image for the PRC which sought to evoke charm and attraction more than fear and hostility around the world. However, Beijing in the 21st century seems to be perceptibly aligning itself with the Machiavellan dictum, "it is much safer to be feared than to be loved".[72] Not entirely giving up on its penchant for seduction, Western observers contend that the PRC seems to be growing "increasingly comfortable with infiltration and coercion: its influence operations have become considerably tougher in recent years."[73]

> Thus, the PRC is said to have modified Joseph Nye's concept of "soft power" and turned it into "sharp power", wherein its resorts to practises associated with "subversion, bullying, and pressure, which combine to promote self-censorship."[74] According to Michael Pillsbury[75], the CCP has derived lessons

---

[72] P. Charon and J.-B. Jeangène Vilmer, *Chinese Influence Operations: A Machiavellian Moment*, Report by the Institute for Strategic Research (IRSEM), Ministry for the Armed Forces, Paris, October 2021.

[73] Ibid.

[74] "What to do About China's 'Sharp Power,'" *The Economist,* 14 December 2017.

[75] Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower,* Henry Holt, New York, 2015, pp. 3, 116.

from its ancient strategic culture, particularly from the Warring States period (475–221 BCE) in its history, which led to the unification of the seven feuding States under the Qin Dynasty. It has derived nine principles of strategy critical to understanding the centrality of its Influence Operations. These are briefly explained below:

- Induce complacency to avoid alerting your opponent.
- Manipulate your opponent's advisers.
- Be patient—for decades or longer—to achieve victory.
- Steal your opponent's ideas and technology for strategic purposes.
- Military might is not the critical factor for winning a long-term competition.
- Recognize that the hegemon will take extreme, even reckless action to maintain its dominant position.
- Never lose sight of Shi (a simple definition for which includes deceiving others to do your bidding for you and waiting for the point of maximum opportunity to strike).
- Establish and employ metrics for measuring your status relative to other potential challengers.
- Always be vigilant to avoid being encircled and deceived by others.[76]

The PRC employs a host of IO activities under the rubric of "unrestricted warfare", the underpinnings of which were published by two People's Liberation Army (PLA) Air Force colonels in February 1999.[77] In the book *Unrestricted Warfare: Assumptions on War and Tactics*

---

[76] Ibid., pp. 35-36.

[77] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization,* PLA Literature and Arts Publishing House, Beijing, 1999.

in the Age of Globalization, the PLA officers write that unrestricted warfare "means that any methods can be prepared for use, information is everywhere, the battlefield is everywhere, and that any technology might be combined with any other technology" and that "the boundaries between war and non-war and between military and non-military affairs has systematically broken down".[78]

THE THREE WARFARES

When the PRC revised the "Political Work Guidelines of the People's Liberation Army" in 2003, the concept of 'three warfares' was introduced. The three warfares consist of psychological/Informational warfare; public opinion and media warfare and legal warfare (or as is popularly known, lawfare).

Psychological/Information Warfare

This involves the planned use of propaganda and other psychological operations to influence the opinions, emotions, attitudes and behaviour of any enemy and at times even friendly country, or an organization/s or group/s.[79]

The People's Liberation Army (PLA) of China currently places great importance on psychological warfare in its military assessments, as it believes that the cognitive domain will be a key domain of future warfare. Although it believes that warfighting in the future will be increasingly AI-driven 'intelligentization', the decisive element would be human decision-making, which means that psy-ops will assume greater significance in gaining influence over adversary leadership, which would have an "outsized impact on conflict." It is for this reason that the PLA has focused on the cognitive domain around "four categories: better understanding the brain, externally controlling the brain,

---

[78] Ibid

[79] Nathan Beauchamp-Mustafaga, , 'Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States',: RAND Corporation, Santa Monica, CA 2023 at https://www.rand.org/topics/psychological-warfare.html (last accessed online on 25 March 2024).

improving one's own cognitive performance, and leveraging the brain for better machines."[80]

According to the RAND Corporation Report titled: *Chinese Next Generation Psychological Warfare*, the PLA is interested in niche technologies for its future operation in psychological warfare, which involves "advanced computing, especially big data and information processing; brain science, especially brain imaging; and a raft of legacy proposals that remain of interest, including sonic weapons, laser weapons, subliminal messaging, and holograms. These technologies can also be combined, such as for cognitive modelling, which appears to be of growing interest."

China's approach to psychological warfare is driven by its view that modern warfare is defined by information and is thus described as *informationized* warfare, with psy-ops dealing in the way adversaries receive and process that information. Thus, psychological warfare is a key part of the larger information warfare process. As the 2006 Science of Campaigns further explains, "inclusion of psychological attack in the scope of information warfare further elevates the direct effectiveness of information operations."[81]

According to PLA's Science of Campaigns of 2006, psychological campaigns include both psychological attacks as well as psychological defence. The goal of psychological attacks is to degrade the adversary's decision-making, weaken the enemy's will to fight, undermine the opponent's support for war, weaken the adversary government from within, along with supporting deterrence. These operations are described as having four key requirements: seizing the initiative, developing specialized command and personnel, employing realistic (tailored) propaganda, and achieving surprise. These Chinese psychological

---

[80] Ibid.

[81] Zhang Yuliang, (ed.), *The Science of Campaigns*, National Defense University Press, Beijing, 2006; *Science of Military Strategy*, (2nd edn.), People's Liberation Army, Academy of Military Science, Military Strategy Department, Military Science Press, Beijing, 2001.

operations are not limited to times of war, but are now interwoven into every domain, both kinetic and non-kinetic, be it in peacetime or during times of conflict and war.[82]

Another set of Chinese psy-ops relate to "psychological defence", which entails developing psychological immunity among the leadership, military and even citizenry. According to Timothy L. Thomas, China is working to "establish the strategic idea of an active psychological-warfare defense (sic). Active defense (sic) should include tempering the minds of the Chinese people by inoculation: allowing the people to come into contact with other ideas and, through education and guidance, allowing them to see what is wrong with those ideas. That approach will allow people to develop psychological immunity. Opening their minds up to other ideas, however, is not the same as cutting them loose."[83]

Among PRC's usual psy-ops IO techniques conducted on a foreign nation or group, are use of diplomatic pressure, rumour mongering, generation and dissemination of fake and false narratives, harassment to express displeasure, assertion of hegemonic claims, and conveying of threats.

Public Opinion Warfare and Media Warfare

According to the 2011 PLA dictionary, public opinion and media warfare refers to "comprehensively using all types of media means and information resources to struggle against the enemy." In the words of Prof. Kerry Gershaneck, China's public opinion and media warfare "involves *weaponizing* all forms of media to shape public opinion in order to weaken its adversaries' will to fight while ensuring strength of will and unity on the Chinese Communist Party's side. To this end,

---

[82] Ibid.

[83] Timothy L. Thomas, 'New Developments in Chinese Strategic Psychological Warfare', Center for Army Lessons Learned, Fort Leavenworth, 2005 at https://apps.dtic.mil/sti/pdfs/ADA434978.pdf (last accessed online on 25 March 2024).

Beijing leverages all instruments that *inform and influence* public opinion, such as social media, newspapers, radio, movies, television programs, books, video games, education systems, and global media networks.'[84]

The Chinese government is often charged with "co-opting individual journalists and media organizations" in Western States. It is said to be adept at conducting *social media warfare* to disseminate a "wide array of propaganda, misinformation, covert disinformation, and fake news".[85] According to Prof, Gershaneck, China employs *Media Warfare in Taiwan and other countries* to undermine their democratic institutions, fracture national unity, demoralize the public and military, and create social instability in pursuit of its goal of annexing this sovereign country.

The CCP has established Chinese Student and Scholars Associations (CSSAs) and Confucius Institutes (CIS) and related programmes. The US alone has roughly 265 CSSAs. Directed by the Chinese Communist Party, these organizations work closely with the Ministry of State Security and United Front organizations in alleged political warfare and influence operations.

According to Prof. Kerry Gershaneck, China employs *online terror and intimidation* through *trolls* who provoke controversy or attack those targeted by the CCP. It also puts up *sock puppets* or fake social media accounts created under false personas that support China's objectives, *bots* that are automated (robot) accounts that amplify information China wants disseminated, to Netizens, and the so-called 50-cent Army as well as the large organizations within the PLA. In fact, China has "more than 2 million Chinese and others are alleged to be members of the "50-cent Army" that manipulates public opinion and attacks PRC critics and other targets. They spread disinformation, create and/or circulate negative propaganda about Taiwan and other

---

[84] 'Democracies still don't understand CCP's political warfare: Kerry Gershaneck,' *The Sunday Guardian*, 27 February 2021 at https://sundayguardianlive.com/news/democracies-still-dont-understand-ccps-political-warfare-kerry-gershaneck (last accessed online on 25 March 2024).

[85] Ibid.

adversaries, propagate fake news, and coerce targeted individuals such as entertainers."[86]

It is alleged that China deceptively *indoctrinates* audiences under the guise of *entertainment* and employs such mediums as movies, soap operas, and video games to convey the CCP's narratives. The Chinese State uses large amount of funds for its propaganda platforms, such as *People's Daily, China Central Television (CCTV), China Global Television Network (CGTN), China Radio International (CRI), China Daily, Xinhua,* and military organizations such as the PLA *News Media Centre* and the *Strategic Support Force*. Conservative estimates point to the fact that funding tops at least tens of billions of US dollars a year. More importantly, China funds private entities such as TikTok that provide applications for censoring smartphones and computers searching for information that China dislikes. [87]

Legal Warfare (also known as Lawfare)

Legal warfare is a part of Influence Operations, which in the words of Elza Kania seeks to exploit "all aspects of the law, including national law, international law, and the laws of war, in order to secure seizing 'legal principle superiority' and delegitimize an adversary."[88] The PRC has sought to assert control over the South China Sea dispute through lawfare the "rather tortuous interpretations of international law to oppose the Philippines' position and seek to delegitimize the arbitration process."[89] It is alleged that China also uses lawfare to block vital US Marine Corps' military activities in Japan and in US Pacific Island territories. China is also seen using minor and flimsy legal loopholes to justify keeping many Pakistani terrorists and terror groups out of the UN list of terrorist groups and individuals.

---

[86] Ibid.

[87] Kerry K. Gershaneck, *Political Warfare: Strategies for Combating China's Plan to 'win Without Fighting'*, Marine Corps University (U.S.). Press, 2020.

[88] Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," *China Brief,* 16 (13), Jamestown Foundation, 22 August 2016.

[89] Ibid.

Active Measures and Sharp Power

Many Western scholars and commentators allege that China resorts to Soviet-style "active measure" tactics, techniques, and procedures, which include deliberately causing street violence, conducting assassinations, carrying out acts of subversion, espionage, blackmail, bribery, deception, enforced disappearances and kidnapping, coerced censorship, and use of proxy forces. It is alleged that the CCP planned an "enforced disappearance" in Thailand to silence an expatriate Chinese critic of the party.[90]

The Chinese diaspora is often characterized by some Western countries as potential unfriendly agents, and it is believed that the PRC views them as a tool to further its political and security interests. It is alleged that Beijing employs various material incentives and means of coercion, along with ideational strategies through information control and targeted propaganda. Chinese government propaganda is said to be directing divisive narratives to its diaspora — such as framing racism and violence as targeted at the diaspora —to divide diaspora communities from host countries. The use of the Chinese diaspora, even Chinese students in Western universities, is alleged, for espionage and subversive activities.

Another form of Information Operation the CCP is charged with, is directed against education systems. The charges range from *controlling the published research* by using sharp power techniques, such as putting pressure on book publishers, printers, and booksellers, co-opting academic advisors, blackmailing and co-opting university officials.[91]

The United States has often accused the PRC of unlawfully attempting to acquire US military technology, trade secrets of US companies as well as classified documents.[92] In addition to traditional espionage, China

---

[90] Kasit Piromya, interview with the author, Bangkok, Thailand, 1 May 2018.

[91] Peter Attis , and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer*. Naval Institute Press, 15 November 2019.

[92] J. Finkle, J. Menn, J.Viswanatha, '*U.S. accuses China of cyber spying on American companies', Reuters News Agency,* 20 May 2014, https://www.reuters.com/article/2014/05/19/us-cybercrime-usa-china-idUSBREA4I09420140519/

is said to use its civilian companies to tie up with American businesses for acquiring technology and economic data[93] and uses cyber espionage to penetrate the computer networks of US businesses and government agencies, such as *Operation Aurora* in 2009 and the Office of Personnel Management Data Breach in 2015. In fact, US law enforcement agencies, like the FBI, often identify China as the most active foreign power involved in illegal acquisition of American technology.[94]

Twin actions of Seduction and Coercion

Through its Influence Operations, China fulfils two principal objectives. The first is to seduce and captivate foreign audiences by presenting a positive narrative of China (glorifying its traditions, benevolence and strength). The second is the even more dubious act of infiltration and coercion.

Infiltration involves slow penetration into the institutions of the targeted society to first forestall any possibility of taking action that may run contrary to the CCP's perceived interests. This coercion may then expand to possible Chinese "punitive" diplomacy that might resort to systematic sanctions against any state, organization, company, or individual that threatens the Party's interests. Both are generally carried out via a web of intermediaries. Overall, these practices target the following categories:

Diasporas, with the dual objective of controlling them – so that they do not represent a threat for the Chinese power. Thus, China is often alleged to carry out a transnational campaign of repression which,

---

[93] Larry M. Wortzel, Hearing on "Enforcement of Federal Espionage Laws." Testimony before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary, US House of Representatives, 29 January 2008.

[94] Jay Solomon, "FBI Sees Big Threat From Chinese Spies; Businesses Wonder". *The Wall Street Journal*, 10 August 2005,ISSN 0099-9660. (last accessed online on 26 March 2024).

according to the NGO Freedom House, is "most sophisticated, global, and complete in the world") – and mobilizes them to serve its interests.

Global Image: It is believed that China has an explicit goal to establish "a new world media order." It is alleged that the government invests €1.3 billion annually since 2008 to impose a tighter control over its global image. The major Chinese media outlets have a global presence, in several languages, on several continents, and on all social networks, including those blocked in China (Facebook, YouTube, and Instagram), and they invest large amounts of money to increase their digital audience artificially. China is also said to control the Chinese-language outlets abroad, which has proven so successful that the CCP now has a near-monopoly among them, and it also seeks to control the mainstream media. Finally, the CCP is said to exert its influence over each step along the global information supply chain, targeting television, digital platforms, and smartphones.

Diplomacy: with a focus on two aspects. China has been charged by Western experts of deploying classic diplomatic resources along with clandestine influence operations (economic and political pressure, co-option, coercion, and corruption) to strengthen its influence. Second, China is said to be employing so-called "wolf-warrior" diplomacy, which refers to more aggressive postures adopted by the Ministry of Foreign Affairs' spokespersons and a dozen diplomats.

Education: universities are one of the main targets of the Party's Influence efforts. Its principal levers are: financial dependence, leading to self-censorship in the universities; surveillance and intimidation of Chinese students, university instructors and administrators on foreign campuses; imposed modifications in course content, teaching materials, or programmed events; and shaping Chinese Studies, by encouraging self-censorship and punishing critical researchers. The Party-State also uses universities to acquire knowledge and technology, via legal and overt means, such as joint research programmes, or illegal and covert actions, like theft and espionage. In a context of civil-military fusion, certain joint programmes or researchers holding positions in dozens of Western universities involuntarily aid Beijing build weapons of mass destruction or surveillance technologies which are used to oppress the Chinese population. On this issue, several scandals broke out in public in 2020 and 2021.

Think tanks: In this case, the Chinese strategy is two-pronged. Beijing seeks to establish overseas branches of Chinese think tanks, and to take advantage of local relays that may themselves be think tanks, with three possible scenarios: occasional partners acting as amplifiers on local markets of ideas, circumstantial allies that spread the Party's narratives, and accomplices that share a common worldview and convergent interests with the CCP.

Culture: China takes the cultural route by producing films, TV series, music, and books – all-powerful tools of seduction. Influence is exerted on foreign filmmakers, for example in Hollywood. To avoid upsetting Beijing and to maintain access to the enormous Chinese domestic market, many American movie studios censor themselves, cutting or modifying movie scenes. Some are even overzealous, casting Chinese characters for "good" roles. Denial of access to the Chinese market is almost certain for any artist who criticizes the Party-State, via other types of pressure. Beijing also hopes to encourage artists to modify their work or, for those exhibiting elsewhere in the world, to simply stop, or even to play the role of Chinese censors.

China and Influence Operations in India

A study by a New Delhi-based think-tank 'Law and Society Alliance' titled "Mapping Chinese Footprints and Influence Operations in India" was published in September 2021. The study claims high penetration of CCP's propaganda across various sectors of Indian cultural and economic sectors — ranging from the Indian entertainment industry (Bollywood, radio broadcasting and music application companies), media, think tanks and civil society, private universities and academic institutions, influence in the tech sector and trade, as well as involvement in disinformation on the social media.[95] However, it is difficult for this Paper to authenticate the claims of these reports.

---

[95] 'Law and Society Alliance study report exposes Communist China's overt, covert influence operations in India', Defence Capital, 04 September 2021 at https://defence.capital/2021/09/04/law-and-society-alliance-study-report-exposes-communist-chinas-overt-covert-influence-operations-in-india/ (last accessed online on 25 March 2024).

In August 2022, a US-based think tank 'New Kite Data Labs' is said to have issued a report that a Beijing-based AI and data collection firm named 'Speech Ocean', collected voice samples from India's sensitive regions, including Jammu & Kashmir, and Punjab. It is alleged that Speech Ocean worked with a New-Delhi based subcontractor who recruited individuals to record their voices in their languages and accents in lieu of small amounts of money. The report underlined that Speech Ocean is known to sell to the Chinese military, and the data collected from India was sold to agencies in China for use and analysis. Indian experts fear that such voice samples could be used for AI-generated, disruptive deep fake videos and audios in the future.[96]

[96] 'China's AI-powered influence operations at India's doorstep', *Hindustan Times*, 06 March 2023 at https://www.hindustantimes.com/ht-insight/chinas-ai-powered-influence-operations-at-india-s-doorstep-101678086529152.html (last accessed online on 25 March 2024).

Chapter IV

Influence Operations: The United States

As the world's sole superpower, the United States plays a prominent role in setting the global agenda on issues of critical importance. Its overwhelming influence is mostly evident in the shaping of key doctrinal and strategic narratives on global issues — be it on the ideological framework of a "global rules based international order" or on the ethical debate on contentious issues of nuclear proliferation, climate change, global trade and finance, human rights or spread of democracy around the world. As the US mostly plays a key role in setting the global agenda, largely inspired by its capitalist, neo-liberal and democratic values and philosophy, other countries and regions mostly respond either in full/partial agreement or outright defiance.

In addition to its overwhelming ideological and strategic influence, the US also pioneers in developing and conducting new forms of overt and covert influence operations, to either convince or coerce countries, blocs and regions to follow its wider geostrategic agenda. In fact, no country comes close to the level of sophistication, scope or extent of multi-pronged influence operations conducted across the globe by the US. However, there is surprising paucity of research literature available on the full extent of influence operations conducted by the US around the world, as the nations and region targeted by its influence operations do not have ample resources or expertise to fully explore and research its influence operations.

US History of Regime Change and Election Interference

It is noteworthy that the US has been involved in conducting coups and in carrying out regime change, even against democratically elected leaders, across the globe since the 19th century. Some of the major

regime changes have been the annexation of Hawaii in 1898 to the installation of dictator Fulgencio Batista in Cuba in 1933 in order to quash revolts that threatened U.S.-owned sugar, fruit and coffee businesses.

When it comes to removing democratically elected leaders, the US holds the dubious record of carrying out the 1953 coup (codenamed *Operation Ajax*) against Iran's elected prime minister Mohammad Mosaddegh, and the CIA-orchestrated coup in 1954 against Guatemala's democratically elected leader, President Jacobo Árbenz, which threatened the interests of the American-owned United Fruit Company, which owned 42 per cent of that country's land territory and still paid no taxes.

The CIA was also involved in the 1960 capture and 1961 assassination of the Republic of Congo's first democratically elected Prime Minister, Patrice Lumumba. The US also was allegedly involved in the coup against elected Chilean President Salvador Allende, and in installing a military dictator, Augusto Pinochet in 1972. In 2003, the United States invaded Iraq and overthrew Saddam Hussein's regime, charging him of having developed weapons of mass destruction.

Still, the US mostly conducted regime change through covert actions; US experts like Lindsay A. Rourke, themselves claim that the country made 64 covert attempts to change regimes during the Cold War.[97] Russia has been blamed for interfering in US presidential elections of 2016 and 2020; *The New York Times* published an article titled: "Russia Isn't the Only One Meddling in Elections, We Do It, Too", by Shane Scoot in 2019, which claimed that the US has either overtly or covertly intervened on at least 81 occasions in foreign elections between 1946 and 2000.[98]

---

[97] Lindsey A. O'Rourke, "The Strategic Logic of Covert Regime Change: US-Backed Regime Change Campaigns during the Cold War". Security Studies, 29, 29 November 2019, pp. 92–127.

[98] Scott Shane, "Russia Isn't the Only One Meddling in Elections, We Do It, Too", *The New York Times*, https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html (last accessed online on 25 March 2024).

Colour Revolutions and Arab Spring: 'US-Instigated Security Threat'?

Many anti-US governments around the world —Russia, China, Iran, Venezuela, etc. — allege that the US has learnt the art of fomenting, organizing and controlling many largely peaceful, pro-democracy protests that, in the case of colour revolution in Post-Soviet Eurasia (from 2000-2005) and the Arab Spring uprisings (in West Asia after 2011), have led to regime change in authoritarian States.

International geopolitics scholars Paul J. Bolt and Sharyl N. Cross state that, "Moscow and Beijing share almost indistinguishable views on the potential domestic and international security threats posed by colour revolutions, and both nations view these revolutionary movements as being orchestrated by the United States and its Western democratic partners to advance geopolitical ambitions."[99]

In fact, Chinese President Xi Jinping appealed to Russia, India, and other members of the Shanghai Cooperation Organisation (SCO) at the group's annual meeting on 16 September 2022 in Uzbekistan, to cooperate with each other in order to prevent foreign powers from destabilising their countries by inciting "colour revolutions".[100]

Similarly, Russian Defence Minister Sergei Shoigu and Russian Foreign Minister Sergei Lavrov characterize these colour revolutions as US-

---

[99] Paul Bolt, Sharyl Cross, *Emerging Non-Traditional Security Challenges: Colour Revolutions, Cyber and Information Security, Terrorism and Violent Extremism in China, Russia and Twenty First Century Global Geopolitics*, Oxford University Press, 2018.

[100] Raghu Malhotra, 'What are the 'colour revolutions' that China's Xi Jinping has warned against?', *Indian Express*, 18 September 2022 at https://indianexpress.com/article/explained/explained-global/what-are-colour-revolutions-chinas-xi-jinping-warned-8157165/#:~:text=What%20are%20%E2%80%9Ccolour%20revolutions%E2%80%9D%3F,the%20Middle%20East%20and%20Asia. (last accessed online on 25 March 2024).

engineered acts with a clear goal of influencing the internal affairs and represent a new form of warfare.[101]

The 2015 Policy White Paper on "China's Military Strategy" by the State Council Information Office said that, "anti-China forces have never given up their attempt to instigate a 'colour revolution' in this country."[102] In July 2007, Iranian State television released footage of two Iranian-American prisoners, both of whom work for Western NGOs, as part of a documentary called *In the Name of Democracy*. The documentary focuses on colour revolutions in Ukraine and Georgia. It accuses the US of attempting to foment a similar ouster in Iran.[103]

These States posit that instead of launching military operations against them, the US instigates protests as a means to subvert regimes and governments to expand its control and influence globally. They claim there is a particular pattern in the way colour revolutions and Arab Spring protests develop and unfold, be it the 'Rose Revolution' in Georgia in 2003, the 'Orange Revolution' in Ukraine in 2004, the 'Tulip Revolution' in Kyrgyzstan in 2005, or the 'Arab Spring' in West Asia and Africa in 2011, all of which desired a pro-American democratic form of governance. However, China's *Global Times* notes, "What colour revolutions left in their wake are neither peace nor Western democracy, but mass confusion, chaos, and destruction in the target countries."[104]

---

[101] Dmitry Gorenburg, "Countering Colour Revolutions: Russia's New Security Strategy and its Implications for U.S. Policy", Ponars, Eurasia, https://www.ponarseurasia.org/new-policy-memo-countering-color-revolutions-russia-s-new-security-strategy-and-its-implications-for-u-s-policy/, 15 September 2014.

[102] Paul J. Bolt, Sharyl N. Cross, "Emerging Non-Traditional Security Challenges: Colour Revolutions, Cyber and Information Security, Terrorism and Violent Extremism", in Paul J. Bolt and Sharyl N. Cross (Eds.), *China, Russia, and Twenty-First Century Global Geopolitics*, Oxford University Press, 2018.

[103] "Iran shows new scholars' footage". BBC News, 19 July 2007.

[104] 'GT Investigates: US Wages Global Color Revolutions to Topple Govts for the Sake of American Control', *Global Times*, 02 December 2021 at https://www.globaltimes.cn/page/202112/1240540.shtml (last accessed online on 25 March 2024).

The patterns behind these popular revolts are that they are led by groups that scrupulously conduct non-violent protest, allegedly following the Gandhian scholar Gene Sharp and his books, *The Politics of Non-Violent Action, Gandhi as a Political Strategist,* etc.[105] Russia and Chinese sources often blame American NGOs, particularly the National Endowment for Democracy, for 'radicalising' groups and providing them information and financial support to intensify their mass mobilisation efforts. Once the efforts reach a critical mass, the NGO and social media groups (along with US mainstream media) organise a chain of protests and generate publicity to cause social discontent to gain traction. Thus, the Chinese government mouthpiece *Global Times* once claimed: "As of 2016, NED (the US NGO National Endowment for Democracy) had provided some $96.52 million to at least 103 anti-China entities, including notorious separatist groups."[106]

US Economic Warfare: Triadic Sanctions, Stock Market Manipulation

The US has been criticised for excessively resorting to punitive economic measures as a means to influence and coerce States into accepting its policies. It is known for frequently imposing economic sanctions, freezing capital assets, suspending aid, prohibiting investment and capital flows, practising tariff discrimination against its adversarial States and even those that trade with them.

It is often argued that far from being an alternative to war, economic sanctions have become a US tool of war and are intended to coerce and even topple governments disfavoured by the US. In reality, sanctions inflict suffering on civilian populations that are not responsible for the actions of their governments but which lead to humanitarian disasters.

---

[105] Michaud, Hélène "Roses, cedars and orange ribbons: A wave of non-violent revolution". *Radio Netherlands*, 29 June 2005.

[106] 'GT Investigates: US Wages Global Color Revolutions to Topple Govts for the Sake of American Control', *Global Times*, 02 December, 2021, https://www.globaltimes.cn/page/202112/1240540.shtml**,** (last accessed online on 25 March 2024).

According to Kaushik Basu, former chief economist of the World Bank and chief economic adviser to the Government of India, the US is an exponent of 'triadic sanctions' and imposes it in an unethical manner even against non-belligerent countries. In 1973, for example, US President Richard Nixon cut off food aid to Bangladesh in the middle of a famine on the grounds that the country was trading with Cuba.[107]

However, in today's high frequency algorithmic trading markets, the dangers of covert cyber operations engineering stock market crashes have increased. Incriminating risk assessment reports by US private research firms can bring down stocks of important corporations and affect stock markets of developed nations overnight. Currency wars and derivatives trading can skew global markets and cause major financial disruptions.

Speculative traders like George Soros, have earned a dubious international reputation of bringing down foreign currencies and central banks with impunity. Dubbed a philanthropist, the nonagenarian Soros is blamed for the collapse of the UK Central Bank — The Bank of England — in 1992 because he short-sold US$ 10 billion worth of Pounds that made him a profit of US$ 1 billion. He has also been accused of playing a role in speculative attacks on Thailand's currency (baht) in 1997, and is linked with the financial crisis in Asia that year. Former Malaysian Prime Minister Mahathir bin Mohamad, blamed him for the devaluation of the Ringgit.[108]

---

[107] Kaushik Basu, 'The New Art of Economic Warfare and the Global Need to Regulate it', *The Mint,* 30 March 2022 at https://www.livemint.com/opinion/online-views/the-new-art-of-economic-warfare-and-the-global-need-to-regulate-it-11648659394026.html (last accessed online on 25 March 2024).

[108] Anil Sasi, 'Who is George Soros, the billionaire that India both attacks and partners with?', *Indian Express,* 11 April 2023 at https://indianexpress.com/article/explained/explained-economics/soros-the-man-his-activities-8452031/ (last accessed online on 25 March 2024).

US MEDIA MANIPULATION: 'MANUFACTURING CONSENT'

Busting the myth that the US media is fair and independent of State influence and of transnational capitalist interests, Edward S. Herman and Noam Chomsky argued in their 1988 book, *Manufacturing Consent: The Political Economy of the Mass Media.*[109] The book argues that the so-called independent media of the US caters to the financial interests of the owners of these publications, such as Corporations and controlling investors. They are also influenced by advertisers who fund the media organizations, rather than the average reader or the citizenry that the media seeks to enlighten.

Again, the large US bureaucracies that are willing to supply steady flow of news to the media organizations and promote their interests through government permits to their business ventures, wield inordinate influence on the message disseminated. Therefore, the US media inadvertently becomes the organ of big business and the State and puts forward news and opinions that promote the interest of the high and mighty, thus manufacturing views and opinion that the readership unwittingly accepts, as coming from an independent source.

Similarly, the book by *Danny Schechter*, *Embedded-Weapons of Mass Deception: How the Media Failed to Cover the War in Iraq,* alleged that major US media conglomerates like CNN were complicit in promoting the war-like agenda of the Bush administration after 9/11 and literally embedded themselves with the military at the time of the Iraq war.[110]

The growing disenchantment of the US audience with mainstream news networks can be measured by the success of RT News and Al-Jazeera increasing their reach in the Western world in recent decades.

---

[109] E. Herman and N. Chomsky, *Manufacturing Consent: The Political Economy of The Mass Media*, Pantheon Books, New York, 1988/2002.

[110] *Danny Schechter*, *Embedded-Weapons of Mass Deception: How the Media Failed to Cover the War in Iraq*, Prometheus Books, 2003.

Exploitation of Religious Conflicts

Russia and China have started accusing US of interfering and exploiting religious factions for political purposes for the purpose of weakening its adversaries and achieving its political power and economic objectives.

For instance, Russian Foreign Minister Sergei Lavrov blamed the US in November 2019 for the split in the Ukrainian Orthodox Church, when it declared itself independent of the Russian Orthodox Church, thus breaking off its centuries-old ties. [111] Similarly, China blames the US for supporting the infamous Falun Gong sect, which it claims is under the alleged influence of the National Endowment for Democracy (NED), and receives large amounts in funding.[112]

Similarly, China blames the US for meddling in the international human rights arena through the annual release of the so-called *International Religious Freedom Report,* which serves the interests of the US government.[113]

Russian and Syrian officials have on several occasions questioned the links between US officials and ISIS militants. In June 2017, Russian Foreign Ministry spokesperson Maria Zakharova said that her country has many questions about unmarked helicopter flights over the areas of activity of ISIS militants, especially in northern Afghanistan. "We've taken note of new reports about unmarked helicopters ferrying the

---

[111] 'US sets itself goal to destroy the unity of world Orthodox Christianity, Lavrov says', TASS (Russian News Agency), 30 August 2021 at https://tass.com/politics/1331801 (last accessed online on 25 March 2024).

[112] James R. Lewis, Junhui Qin, "Is Li Hongzhi a CIA Agent? Tracing the Funding Trail Through the Friends of Falun Gong," *Journal of Religion and Violence*, Philosophy Documentation Center, 17 February 2021 at https://www.pdcnet.org/jrv/content/jrv_2021_0999_2_16_80 (last accessed online on 25 March 2024).

[113] 'GT Investigates: US cultivates pseudo-religious groups overseas, pumps support to terrorists to wreck its adversaries', *Global Times*, 06 December 2021 at https://www.globaltimes.cn/page/202112/1240827.shtml (last accessed online on 25 March 2024).

fighters of ISIS Afghan branch, as well as weapons and munitions for them, in eastern Afghanistan," Zarakhova reportedly said.[114]

Thus, US' championing of religious belief appears to have gone beyond its professed adherence of human rights and swings towards interventionism.

[114] 'Russia Questions Reports of Unidentified Helicopters Sighted in Afghanistan', *Ariana News*, 23 June 2017 at https://www.ariananews.af/russia-questions-reports-of-unidentified-helicopters-sighted-in-afghanistan/ (last accessed online on 25 March 2024).

Chapter V

Influence Operations: Pakistan

Pakistan is not a typical nation state. Although it has a people inside a certain geographical limit, its national ethos does not necessarily come from within its territory's history, language and culture, but springs from a transnational religious revivalist outlook, which makes it more of a revisionist and revolutionary State rather than a conventional nation state. Therefore, influence operations play a key role in Pakistan's ideologically and politically motivated worldview.

Pakistan was born out of the Islamist ideology of the poet-philosopher Muhammad Iqbal. It was his dream to establish an ideal Islamic State for reviving the glory of the Muslim world at least in the subcontinent that stirred the Jinnah-led Muslim League into creating Pakistan by partitioning India in 1947.

The Role of ISI and ISPR

This ideological fervour later got a further dose of radicalism when Abul Ala Al Maududi, regarded as the Karl Marx of Political Islam, migrated to Pakistan from India and put forward a Shariah-driven political model for running an Islamic State in the modern world.

The war against Soviet Union further intensified the Islamization drive and Pakistan became the epicentre of violent extremism and terrorism. The influx of radical Arab mercenaries, helped by the Pakistan military and ISI fighting in Afghanistan in the 1980s, exacerbated the situation. Pakistan became the breeding ground for Islamist and jihadist radicalisation, which it launched primarily against India (particularly in Jammu and Kashmir) as well as on the rest of the world.

This study does not have the length and scope to fully discuss the ideology, methodology, strategic and end-state goals of Pakistan's revolutionary brand of political Islam disseminated through its IO

methods, and with the collusion of ISI and transnational Islamist ideologues as well as jihadist groups over the decades.

Formed in 1948, Pakistan's Inter- Services Intelligence (ISI) is the best-known agency of Pakistan intelligence community. Its Covert Action Division engages in activities similar to 'Active Measures" infamous in Soviet times, even though some of its officers received training from the CIA's Special Activities Division in the initial years.[115] It is active in various countries such as Afghanistan, India, Iran, Iraq, the US, the UK, Libya and several countries in West Asia, Central Asia and Africa.

The Inter-Services Public Relations (ISPR) is the public face of the ISI and a major arm of its IO-like operations. Established in 1949, it is essentially Pakistan Army's media and public relations wing. Despite being attached to the military, the ISPR broadcasts televised news on a regular basis and provides updates on the Pakistan Army's strategic operations in foreign and domestic areas.[116]

The organization is said to have a 'three-tier structure' for its propaganda operations. The first tier comprises writers, authors and academicians who build positive meta-narratives for the State, mainly the Army. The second-tier conducts talent spotting workshops, competitions and seminars to spot young researchers at educational institutions, who then work as interns at the ISPR, after which they are left to pursue jobs in the country or abroad and these students eventually become life-long associates of the ISPR. Over a decade, the ISPR has raised an astonishing network of 4000-strong highly qualified Information Warfare Specialists through a carefully crafted internship programme directly run by the ISI.[117]

---

[115] B. Raman, *Intelligence: Past, Present and Future,* Lancer Publishers & Distributors, New Delhi, 2002.

[116] John Adache, *The Military and Public Relations*. AuthorHouse Publications, Bloomington Indiana, 2014.

[117] Jiten Jain and Saroj Rath, 'Information Warfare: Why India needs to give Pak propaganda machinery a taste of its own medicine', *Daily O*, 24 August 2020.

The third tier covers people from mainstream media (television anchors, film personalities, theatre actors etc). It also includes people from the video and mobile games industry, as well as social media personalities.[118]

This association helps ISPR wage comprehensive and coordinated public relations campaigns; for example, against Indian agencies in Jammu and Kashmir, and to send violent and radical extremist messages. The organization helps build national narratives promoting the ideology of the State, events and developments.[119]

Radical Radio, Television, Social Media Channels Targeting J&K

In its 2020-edition, the *Pakistan Army Green Book* unabashedly stressed the need for engaging with India in the "non-kinetic" domain.[120] Former Pakistani Maj Gen. Asif Ghafoor frequently underscores the ISPR's need to pursue the fifth-generation warfare by employing thousands of trolls, who disseminate messages that are pro-Army, Muslim, pro-Kashmir, and patriotic.

ISPR runs many radio channels without licence to disseminate fake news, which shut down frequently and are soon replaced by others. Broadcasting disinformation, these channels operate anonymously to allow deniability. According to a report in *The Tribune*, Pakistan has setup at least 15 round-the-clock FM stations that hurl invectives at India and conduct psychological warfare in Jammu and Kashmir and Punjab.[121] Pakistan's anti-India radio channels that can be heard in the

---

[118] Jyoti M. Pathania, *Deep State Continuum in Pakistan and Implications for India*, KW Publishers, New Delhi, 2022.

[119] "How many radio stations, journalists work for you? Asma Jahangir asks ISPR". *Daily Pakistan Global*, Retrieved 22 December 2017.

[120] *Pakistan Army Green Book*, 2020 at http://syklibrary.ndu.edu.pk/libmax/opac/PeriodicalDetail.aspx?id=11168

[121] 'Pakistan's psychological war on through 15 FM stations', *The Tribune*, 21 November 2018 at https://www.tribuneindia.com/news/archive/j-k/pakistan%E2%80%99s-psychological-war-on-through-15-fm-stations-686928 (last accessed online on 25 March 2024).

Kashmir region are: Radio Buraq FM 104-105 MHz, Radio Swat Network 100 FM and Voice of Kashmir 95.8 FM.[122]

Pakistani propaganda is also received through illegal satellite television operators in Jammu and Kashmir, with at least 50 Saudi and Pakistan TV channels streaming into Kashmiri homes daily. These channels include banned channels like Zakir Naik's Peace TV and other radical Salafi and anti-India channels.[123] Banned Pakistani channels include Madani Channel, Hadi TV, Dawn News, etc. ISPR modus operandi includes creation of camouflage groups on WhatsApp, Facebook, Snapchat applications. Pakistan Army's monthly magazine *Hilal* has five versions (*Hilal* English, *Hilal* Urdu, *Hilal for Her*, *Hilal for Kids* Urdu), which are replete with Pakistani propaganda material.[124] The speeches of UN designated terrorists like Masood Azhar are easy to access on websites like YouTube, leaving the Dark Web for more insidious recruiting and training purposes.

Madrassa Radicalisation and the Terror Threat

The ISI's disruptive activities in its near abroad, particularly India, is far more pernicious than the international community, or the Western media seems ready to accept. For instance, the network of 'jihad-factory' madrassas is not limited to the Af-Pak region alone, which continues to spew venom into Jammu and Kashmir and northern states of India, but its ability to radicalise is as dangerous and pernicious in its influence in southern and eastern states of the country as well.

In 2019, the National Investigation Agency (NIA) had warned that Jamaat-ul Mujahideen Bangladesh (JMB) is trying to spread its tentacles

---

122 Rajesh Bhat, *Radio Kashmir: In Times of Peace and War*, Stellar, 2018.

123 "Pakistani, Saudi Channels Beam into Kashmiri Homes, Stoke 'Azadi Rage'", 5 May 2027 at http://timesofindia.indiatimes.com/articleshow/58524303.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last accessed online on 25 March 2024).

124 Jyoti M. Pathania, *Deep State Continuum in Pakistan and Implications for India*, KW Publishers, New Delhi, 2022, pp.123-17.

across Jharkhand, Tamil Nadu, Maharashtra, Karnataka, Kerala and Bihar.[125] It is noteworthy that JMB has very close links with Pakistan intelligence agencies and Lashkar-e-Taiba. In two separate incidents reported in 2015, JMB was found receiving finances from officers at the Pakistan High Commission in Dhaka. A Visa Attache, Mazhar Khan, was caught red-handed at a meeting with a JMB operative in April of that year, and is said to have been pushing large consignments of fake Indian currency into West Bengal and Assam.[126]

In fact, these radical groups are involved in cattle smuggling, fake currency circulation, drugs and arms peddling across large areas of the border which is unfenced. [127] In its reply to a question in Parliament in July 2019, the Home Ministry said that madrassas in Burdwan and Murshidabad districts of West Bengal were radicalising and recruiting local youth.[128] Many of these seminaries are reportedly teaching radical concepts of 'qital' (warfare), the need for establishment of the Caliphate and the need to fulfil the *Ghazwatul Hind* controversial/'forged' prophecy.

In a similar manner, Indian intelligence sources point to ISI funding large number of mosques and madrassas rising in a 10-km stretch on the India-Nepal border. It is reported that while the number of mosques have gone up from 760 in 2018 to 1,000 in 2021, the number of

---

[125] 'Jamaat-ul Mujahideen Bangladesh trying to spread tentacles across India: NIA chief' *Economic Times,* 14 October 2019 at https://economictimes.indiatimes.com/news/defence/jamaat-ul-mujahideen-bangladesh-trying-to-spread-tentacles-across-india-nia-chief/articleshow/71579100.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (last accessed online on 25 March 2024).

[126] ""Terror financing': Pak diplomat withdrawn from Bangladesh", *The Daily Star,* 23 December 2015.

[127] "Fake Indian Currency Note racket in Bangladesh", *Dhaka Times,* 3 March 2015.

[128] Sujit Nath, 'Jamaatul Mujahideen Bangladesh Using Madrassas in Bengal for Radicalisation of Youth: Home Ministry', News 18, 2 July 2019.

madrasas have risen from 508 in 2018 to 645 in 2021 in the Nepali territories.[129] Similarly on the Indo-Bangladesh border, over 500 madrassas operate in 22 bordering districts of West Bengal. The menace of jihadist propaganda online has spread in southern states as well, including in Kerala, Tamil Nadu, Karnataka and Orissa. But the threat of Islamist radicalisation in the education sector has also seeped into school, college and university-level education in Jammu and Kashmir, with the more intellectually inclined Jamaat-e-Islami ideologues, serving as professors and officials, often serving as Over Ground Workers (OGWs) and 'hybrid militants' for secessionist forces.

ISI covert operations in Punjab, Northeast and Other States

Pakistani disruptive propaganda is not restricted to jihadist radicalisation alone, but it even caters to other secessionist causes in India. In 2021, a disinformation network based in Pakistan spread polarising narratives about the Mizoram-Assam border clashes. A small cluster of Twitter accounts, using similar images and hashtags, openly coordinated activities to stoke religious and political tensions between the two states.

The accounts amplifying this messaging – Mustnowit (now suspended), Usama, and Sharazi – have actively been using the hashtag #FreeAssam along with other hashtags such as #FreeMizoram, #FreeNagaland, #FreeTamilnadu. The accounts were actively spreading disinformation about India, and have tried to capitalise on incidents of religious violence taking place in the country. The campaign is largely being carried out by IT professionals based out of Pakistan.[130]

Similarly, ISI operatives from Pakistan heavily oversee the internet presence of elements spreading Pro-Khalistani content. The posts related to the incidents of the militancy era have generated a renewed fondness

---

[129] 'ISI-funded mosques, madarsas on India-Nepal border raise serious security concerns', *India Military Review*, 6 February 2022 at https://imrmedia.in/isi-funded-mosques-madarsas-on-india-nepal-border-raise-serious-security-concerns/ (last accessed online on 25 March 2024).

[130] Atandra Ray and Dhriti Kamdar, 'Pakistan-Based Disinformation Op Focuses on Mizoram-Assam Border', *Logically??*, 12 November 2021 at https://www.logically.ai/articles/pakistan-based-disinformation-op-focuses-on-mizoram-assam-border (last accessed online on 25 March 2024).

for Bhindranwale and his actions. Babbar Khalsa International's Wadhwa Singh Babbar, who leads the organization from Lahore and is responsible for the assassination of former Punjab chief minister Beant Singh is suspected of using drones to smuggle weapons across the border into India and playing a key role in raising funds by getting in touch with like-minded individuals and organizations in the West. In its attempt to recruit youth on social media, ISI has formed an outfit, Lashkar-e-Khalsa, under its K2 (Kashmir-Khalistan) desk.[131]

Through this group, ISI is facilitating and promoting pro-Khalistan propaganda among pilgrims visiting Pakistan through the Kartarpur Corridor. Although the Corridor was exclusively established for pilgrimage purposes, Indian intelligence agencies report the constant presence of ISI agents and Pakistan Intelligence Bureau officials along their side of the Corridor.[132]

Indian diplomatic missions in the West would have to be alert about growing Pakistani support for pro-Khalistani groups in the West. It is noteworthy that Pakistan's Consul General Janbaz Khan visited two pro-Khalistan gurudwaras in the Surrey suburb of Vancouver in September 2022, ostensibly to thank the office-bearers for their donations to flood relief in Pakistan.

However, the timing of the visit to the pro-Khalistan gurudwaras coincided with the so-called "Sikh Referendum" held on 18 September by extremist elements in Brampton, Ontario.[133]

---

[131] Raj Shekhar, "ISI has new outfit manned by Khalistani, Kashmiri ultras: Intel," *The Times of India, 11* May 2022 at https://timesofindia.indiatimes.com/india/isi-has-new-outfit-manned-by-khalistani-kashmiri-ultras-intel/articleshow/91481883.cms. (last accessed online on 25 March 2024).

[132] Mukesh Ranjan, "Intelligence: ISI misusing Kartarpur Corridor," *The Tribune, 4* May 2022 at https://www.tribuneindia.com/news/punjab/intelligence-isi-misusing-kartarpur-corridor-391857 (last accessed online on 25 March 2024).

[133] Rajinder S. Taggar, 'Top Pak diplomat holds secret meeting with Sikh radicals in Canada to fuel anti-India movement,' *India Narrative,* 23 September 2022 at https://www.indianarrative.com/world-news/top-pak-diplomat-holds-secret-meeting-with-sikh-radicals-in-canada-to-fuel-anti-india-movement-52783.html (last accessed on 17 April 2024).

Chapter VI

Influence Operations by Non-State Actors

Influence Operations by Non-State Actors

In addition to the geopolitics of nation states, the international system consists of a host of international organizations, and private actors. Since the Second World War, many international organizations have emerged, as economic, political, social and cultural transactions between individuals, societies and States have increased.

However, the rise of these non-State actors has inhibited "state-centric" nature of international politics and replaced it with a "transnational" system, which has made intra-regional relations more complex.

These non-State actors and organizations have brought about a sea change in the international environment and new theories of International Relations have been developed, with novel concepts like "complex interdependence" (as proposed by Robert Keohane and Joseph Nye in 1989) becoming popular.[134] C. W. Kegley and E. R. Wittkopf (1995) point out that "as the world grew smaller, the mutual dependence of nation-states and other transnational political actors on one another has grown".[135]

---

[134] R. O. Keohane and J.S. Nye, '*Power and Interdependence: World Politics in Transition',* Harper Collins Publishers, Second Edition, New York, 1989.

[135] C. W. Kegley and E. R. Wittkopf (eds.), *The Global Agenda: Issues and Perspectives*, McGraw-Hill, Inc., New York, 1995, p. 92.

According to S. Brown, non-State actors can be divided into two categories: international inter-governmental organizations (IGOs) and transnational or international non-governmental organizations (NGOs).[136] *International Inter-governmental Organizations (IGOs)*

International Inter-governmental Organizations (IGOs) are voluntary associations of sovereign States that pursue diverse objectives with a formal structure.[137]

IGOs are adjuncts of nation-states and play significant roles by providing means of cooperation and multiple channels of communication among States. IGOs may be classified by scope (global and/or regional) and/or by function (political, economic, social and environmental).

It is well known that the main functions of IGOs is rule making, agenda setting, and information gathering. In addition, they decrease uncertainty between States and search for cooperative solutions for international problems. IGOs may change norms of International Relations and preferences of nation-states. For instance, the United Nations Environment Programme played a significant role in the creation of regimes such as the Protection of the Mediterranean Sea and the Protection of Ozone layer.[138]

The most well-known example of an IGO is the International Atomic Energy Agency (IAEA), which monitors the "non-proliferation of atomic weapons" principle in States whenever any claim is made. They decrease the cost of information gathering which is more important for poor and small countries. For example, the UN plays a key role for States – small States in particular – in receiving information about

---

[136] S. Brown, *New Forces, Old Forces, and the Future of World Politics*, Post-Cold War Edition, Harper Collins College Publishers, New York, 1995.

[137] L. H. Miller, *Global Order: Values and Power in International Politic,* Westview Press, Boulder CO, 1994.

[138] M. Ataman, "The Effectiveness of International Organizations," Abant Izzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, v. 2000-1, no. 1, pp. 152-167.

international politics and systemic issues. Without the UN, many States would be unable to obtain information about the international society and politics. Activities of IGOs, such as the UN and the IMF, are decisive for most small countries. They may impose their principles on them more easily than on big powers.

Unfortunately, powerful States are less constrained by the influence of IGOs, for better or for worse, than those who are relatively weak. The IMF and the UN Security Council are two prominent organizations, which some developing nations allege, impose their principles selectively. For instance, the UN Security Council cannot accept any decision against the interests of the five permanent members and those of their allies.

The influence of IGOs varies with the capacity of governments of member states to implement their own provisions. For example, the IMF and the World Bank are very effective in flow of funds, debt management and financing debt between the developed and developing. Still effective, IGOs have proven least successful on political and security issues.

NON-GOVERNMENTAL ORGANIZATIONS (NGOS)

Non-Government Organizations (NGOs) are institutions that are established by non-state actors, in part or completely. Coming in various forms, NGOs can be transnational, government organized, government-regulated and initiated, business and industry related, donor-organized, donor-dominated, people's organizations, operational, advocacy, transnational social movements, quasi, and anti-governmental NGOs. Their numbers have been on the increase and their effectiveness for transnational politics has gained greater relevance in recent decades. They have become "crucial participants in the international policy process"[139]and their formal and informal power and influence strongly affects the policies of governments around the world.

---

[139] S. Brown, *New Forces, Old Forces, and the Future of World Politics*, Post-Cold War Edition, Harper Collins College Publishers, New York, 1995.

Non-governmental organizations work at a variety of levels at the national, international and transnational levels and are often influenced by special interest groups in the public or private sectors. Human rights advocates, gender activists, religious movements, developmentalists, and indigenous peoples are some of the key areas of International Relations, in which the role of NGOs has significantly increased in recent decades. According to Brown, "as the countries and sectors of world society have become more and more interdependent, it has become commonplace for non-governmental groups representing similar communities in their various countries to closely coordinate their policies and to constitute (or reconstitute) themselves as international non-governmental organizations (INGOs)".[140] The role and influence of these groups, both for good and at times nefarious purposes, has made them critical constituents of influence operations launched by big corporations, governments and special interests, often covertly guiding the affairs of such organizations.

Again, NGOs refer to all kinds of non-governmental organizations. Thus, they not only include multinational corporations (MNCs), but even national liberation movements (NLMs), epistemic communities, religious and humanitarian organizations, even trans-national terrorist groups and drug traffickers, which have a significant impact on international geopolitical and geo-economic levels.

a) Malefic Influence of Multinational Corporations (MNCs)

The most prominent contemporary NGOs are multinational corporations (MNCs).[141] The term usually refers to huge firms that own and control plants and offices in more than one country and sell

---

[140] Ibid., p. 267.

[141] S.D. Krasner, "Power Politics, Institutions, and Transnational Relations," in Thomas Risse Kappen (ed.) *Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures and International Institutions,* Cambridge University Press, Cambridge, 1995, pp. 257-279.

their goods and services around the world. In the neo-liberal globalized order, MNCs are seen as "major driver of global economic integration" and "establish unprecedented linkage among economies worldwide".[142]

Today, the biggest and the most influential corporations are based in the United States, Europe, Japan and China. In 1992, of the 20 largest MNCs, excluding trading companies, in terms of sales were based in G-7 States – eight in the United States, four in Japan, three in Germany, and five in Britain, and two were jointly based in the Netherlands.[143]

MNCs can be classified according to the kinds of business activities they pursue such as extractive resources, agriculture, industrial products, transportation, banking, and tourism. The most notable MNCs are industrial and financial corporations (the most important being banks). Naturally the primary objective of MNCs is profit maximization.[144] They are very effective in directing foreign policy of states, including that of the most powerful ones, and they set agenda for international politics. They have become a major factor in the national economic decision-making process. As mentioned by Miller, the activities of MNCs, "may seem evidence of the growing inability today of the sovereign state to control and regulate effectively economic activities within the private sector. If that is so, then one of the traditional rationales for modern sovereignty is undermined".[145]

One of the measures of the influence of MNCs is the extent of the resources they control. They have enormous "flexibility in moving goods, money, personnel, and technology across national boundaries,

---

[142] E. R. Peterson, "Looming Collision of Capitalisms?" in Charles W. Kegley, Jr. and Eugene R. Wittkopf (eds.) *The Global Agenda: Issues and Perspectives,* McGraw Hill, Inc., New York, 1995, pp. 259-269.

[143] J. S. Goldstein, *International Relations,* Third Edition. Longman, New York, 1999, p. 415.

[144] M. Miyoshi, "A Borderless World? From Colonialism to Transnationalism and the Decline of the Nation State," *Critical Theory*, 19 (4), 1993, p. 746.

[145] L. H. Miller, *Global Order: Values and Power in International Politic,* Westview Press, Boulder CO, 1994,p. 67.

and this flexibility increases their bargaining power with governments".[146] Dozens of MNCs have annual sales of tens of billions of dollars each. Many of them generate more economic activity than the GDPs of most states in the world.

For instance, MNCs such as General Motors, Exxon, Royal Dutch Shell, General Electric and Hitachi outranked the GDP of Taiwan, Norway, Turkey, Argentina, Pakistan, Malaysia and Nigeria in the early 1990s.[147] As compared "to total world export in 1992 of about $4.0 trillion", "sales by MNCs outside their countries of origin were $5.5 trillion for the same year".[148]

Favourable and Unfavourable Views on the Role of MNCs

MNCs are viewed differently by different economic schools of thought. For liberalism, MNCs stand at the vanguard of the new world order as they possess the most efficient means of production.[149] Liberal economists argue that "the global efficiency and the increased generation of the wealth result from the ability of MNCs to invest freely across international borders".[150] Some of these liberal economists even welcome the prospect of MNCs replacing the nation-state as the main economic unit.[151]

---

[146] A. L. Bennett, *International Organizations: Principles and Issues*, Prentice Hall, Englewood Cliffs NJ, 1991, p. 264.

[147] S. Brown, *New Forces, Old Forces, and the Future of World Politics*, Post-Cold War Edition?, Harper Collins College Publishers, New York, 1995, pp. 153-54.

[148] E. R. Peterson, "Looming Collision of Capitalisms?" in Charles W. Kegley, Jr. and Eugene R. Wittkopf (eds.) *The Global Agenda: Issues and Perspectives,* McGraw Hill, Inc., New York, 1995, p. 262.

[149] K. Mingst, "Essentials of International Relations," W. W. Norton & Company, Inc., New York, 1999, p. 223.

[150] J.S. Goldstein, *International Relations,* Third Edition. Longman, New York, 1999, pp. 415.

[151] R. J. Barnett and J. Cavanagh, *Global Dreams: Imperial Corporations and the New World Order*, Simon and Schuster, New York, 1994, pp. 19-20.

Meanwhile, mercantilist and nationalist perspectives take a more ambivalent view and argue that MNCs are instruments of their home States. For them, MNCs either serve national interests of the State or become a threat to the State.[152]

On the other extreme is the Marxist tradition, which considers MNCs as the instrument of exploitation and as an extension of the imperialism of strong capitalist States. According to Marxists, the monopolistic power of the MNCs causes uneven development and inequality in the international division of labour.

The fact is that MNCs present us with a mixed bag. When we observe activities of MNCs, we find that their operations create both opportunities and problems for home countries – States where the MNC have their headquarters and host countries – States in which a foreign MNC operates.[153]

An observer calls the relationship between MNCs and host countries as a 'love-hate' syndrome; as host countries may have both advantages and disadvantages in their relations with MNCs. On the one hand, MNCs are considered instruments of economic development for developing countries, but they may also challenge State sovereignty of the host countries and the latter's control over their economies may be diluted or eroded. They may create political and social division and prevent the development of domestic industries in host countries.

Meanwhile, MNCs may serve the national interests of home countries as instruments of global economic development, a mechanism for spreading ideology, political influence and serve as a tool of diplomacy, particularly sharp power. One should bear in mind that MNCs have a highly centralized set-up and are dominated by the parent company, which is located in the home country.

---

[152] K. Mingst, *Essentials of International Relations*, W. W. Norton & Company, Inc., New York, 1999, p. 224.

[153] M. Carnoy, "Multinationals in a Changing World Economy: Whither the Nation-State," in M. Carnoy et. al. (Eds.) *The New Global Economy in the Information Age*, Pennsylvania State University Press, University Park PA, 1993, pp. 63-65.

The administrators are often from the home country, their research is centralized, the technology is imported from the home State, "profits are often repatriated, and the policies of the firm conform closely to the economic and foreign policies of the home government".[154] Therefore, some, i.e., dependency theory, consider MNCs as instruments for colonization.

International Organizations for Political, Economic, Social Security and Stability

After the Second World War, nation-states have increasingly taken into consideration international and transnational public opinion in the affairs of governance since there are dozens of transnational organizations that monitor human rights practices of nation-states.[155]

The most notable example of international human rights regime is the United Nations, International Monetary Fund, International Court of Justice, World Health Organization, International Labour Organisation (ILO), The European Commission of Human Rights, etc.[156] Member states are increasingly curtailing their sovereignty to the organization on humanitarian issues. These non-state actors mainly concern about morality, human rights, environment and social values. Out of these, International Red Cross, International Red Crescent, and Amnesty International (AI) are the most well-known and influential NGOs among humanitarian international organizations that monitor human rights worldwide.

---

[154] A.L. Bennett, *International Organizations: Principles and Issues*, Prentice Hall, Englewood Cliffs NJ, 1991.

[155] J. Donnelly, "Human Rights and International Organizations: States, Sovereignty, and the Alternatives", *Turkish Journal of International Relations*, 2 (1), Fall 2003, p. 64; "International Community," in Friedrich Kratochwil and Edward Mansfield (eds.) *International Organization: A Reader*, Harper Collins Publishers, New York, 1994.

[156] Ibid., p. 211.

Terrorist Groups, Narco-Terrorists and Radicalisation as IO

Although national liberation movements (NLMs) and ethnic groups sometimes use terrorism for their objectives, terrorist organizations are different from NLMs. Terrorism is their main means of struggle and liberation, and to claim national territories, though that may not be their sole objective. International terrorism is "the most conspicuous and threatening form" of low-intensity violence.[157] Some States even resort to "State terrorism" against powerless communities or ethnic groups.

While some States like Pakistan orient their policies by supporting terrorist groups, other States alter their foreign policies by taking counter-terrorist measures.

Even though drug traffickers are engaged in a profitable "transnational business," they are similar to terrorist organizations because they infiltrate the civilian population and make them victims of their nefarious activities. They are also prone to carrying out assassinations and kidnappings and often target the young and impressionable members of society. These narco-terrorists often have transnational reach and their activities affect the body politic of the targeted countries. Thus, non-State actors, like terrorists and narcotics dealers pose a significant threat to nation-states and often act in collusion, with narcotics funding weaponry for terrorists and providing them access into enemy territory. These non-State threats have been rightly called "enemies without an address".[158]

It is important to refer here to the process of radicalisation, which can be characterised as an influence operation that many violent extremist and terrorist groups around the world employ to spread their malicious designs.

---

[157] C. W. Kegley and E. R. Wittkopf (eds.), *The Global Agenda: Issues and Perspectives,* McGraw-Hill, Inc., New York, p. 92, 1995.

[158] Bishara, M. "Adresi Belli Olmayan Düsman," Birikim, no. 151, pp. 75-78, 2001.

In the wake of differences over the proper meaning and definition of the term 'radicalisation', various State intelligence agencies and security services have come up with their own 'working definitions' for radicalisation and its related concepts.

Thus, the Dutch Security Service (AIVD) defines radicalisation as "Growing readiness to pursue and/or support—if necessary by undemocratic means—far-reaching changes in society that conflict with, or pose a threat to, the democratic order."[159] Under its CONTEST counterterrorism strategy, the UK's Home Office has referred to radicalisation simply as: "The process by which people come to support terrorism and violent extremism and in some cases, then to join terrorist groups."[160]

The development of radical narratives in itself is a very complex process and is often the handiwork of a particular subset of a political ideology that develops it in a very clinical, straitjacketed and strategic manner, in order to develop the right kind of recruit for the radical cause. For instance, much of Sunni Islamist radicalisation is the product of Salafi-jihadist extremism (to which major transnational jihadist groups like Al-Qaeda and ISIS belong) that details a specific kind of ideology, methodology, lifestyle and end-state for its brand of violent extremist groups so that they do not deviate from their radical path.

Notwithstanding their ideological issues with globalisation, jihadist organisations have made full use of the Internet and social media for spreading their influence worldwide.

In this respect, the so-called 'Dark Web' (part of the World Wide Web not indexed by Web search engines) provides the perfect 'breeding grounds' for the seeds of radicalisation to thrive and grow.

---

[159] Dutch Security Service (AIVD), 2005, cited in Randy Borum, 'Radicalization into Violent Extremism' at http://scholarcommons.usf.edu/ cgi/ viewcontent.cgi?article=1139&context=jss (Accessed on 4 January 2016).

[160] UK Home Office, "CONTEST: The United Kingdom's Strategy for Countering Terrorism", July 2011 at http://tinyurl.com/5rtjqal and www.homeoffice.gov.uk/publications/counter-terrorism/counter-terrorism strategy/strategycontest?view=Binary, (Accessed on 14 January 2016).

Most jihadist groups use the Internet for:

1. Propaganda;
2. Scouting prospective radical recruits from the global throng, otherwise difficult to identify and contact in real world;
3. Indoctrination and radicalisation;
4. Terror financing, mainly through cryptocurrencies;
5. Providing instructions for combat training and weapons manufacturing (particularly from objects of everyday use);
6. Carrying out cybattacks (although incidents of hacking have been few and of relatively very limited impact);
7. Coordinating terrorist attacks; and
8. Marshalling forces during active operations in theatres such as Syria, Iraq and Libya.[161]

Globalised Big Business, Cartels, Hedge Funds, Military-Industries and Private Armies

In recent years, the influence operations allegedly conducted by major global conglomerates and international cartels has been the subject of much speculation, even conspiracy theories. The overpowering influence of the so-called US military-industrial complex, the supposedly intractable Big Pharma, Big Oil, Big Banks (Investment banks Goldman Sachs, J.P Morgan and Morgan Stanley) and now Big Tech on the public policy at the global levels and the rise of private military mercenary groups like the Russian Wagner Group, Academi (formerly Blackwater), G4S Security, etc., are a new set of non-State MNCs,

---

[161] Ines Von Behr, Anaïs Reding, Charlie Edwards and Luke Gribbon, "Radicalization in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism", RAND Europe, 2013 at https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/ RAND_RR453.pdf (Accessed on 25 March 2018).

private armies, etc. who exert greater weight in global affairs today, than is often officially recognised. The aggressive activism of huge hedge funds in international finance and investment can hardly be understated.

i) The Alleged Influence of 'Big Oil'

Big Oil is a label stuck on the world's six or seven largest publicly traded oil and gas companies, also known as supermajors**,** alleged to wield immense economic power and political influence.

The companies frequently mentioned as Super Majors, are Exxonmobile, Chevron, BP, Shell, Eni and ConcoPhilips. The tag "Super-Major" emanated from a Report published by Douglas Terreson of Morgan Stanley in February 1998.[162] The Report foretold a substantial consolidation phase of 'Major' Oil companies, which would result in a group of dominant 'Super-Major' entities.

To this day, Big Oil is often alleged to indulge in deceitful and manipulative practices. As late as 2022, a year-long US House of Representatives investigation uncovered major efforts by Big Oil to deceive the public by creating the wrong impression that these fossil fuel companies were taking steps to move away from fossil fuels as part of an energy transition towards a sustainable future, while internal company documents reveal that they have no such plans. Major findings of the Committee, based on company documents, were that these companies proceeded with plans for long-term fossil fuel production and thus continued to be the primary drivers of global climate change while publicly pledging to transition to renewable energy sources; and launched advertising campaigns targeting the American public, and engaged in accounting gimmicks and delaying manoeuvres, to create the false impression that they are taking major steps to reduce carbon emissions, without actually taking such steps.

---

[162] Christopher Helman, "The World's Biggest Oil And Gas Companies", *Forbes*, 19 March 2015.

ii) Conspiracy Theories linked to Big Pharma

According to Steven Novella, the term *Big Pharma* has come to connote a demonized form of the big pharmaceutical companies, said to influence major States, markets and international organizations.[163]

Its name is often associated with conspiracy theories, which claim that pharmaceutical companies, especially large corporations, act in sinister and secretive ways, such as concealing effective treatments, or even intentionally causing and worsening a wide range of diseases, in pursuit of profitability, or for other nefarious reasons.

Some theories have included the claim that natural alternative remedies to health problems aresuppressed; they claim that drugs for the treatment of HIV/AIDS are ineffective and harmful; they claim that a cure for all cancers has been discovered but hidden from the public, claim that COVID-19 vaccines are ineffective, and that alternative cures are available for COVID-19.[164] In most cases, the conspiracy theorists have blamed pharmaceutical companies' search for profits. A range of authors have shown these claims to be false, though some of these authors nevertheless maintain that other criticisms of the pharmaceutical industries are legitimate.

iii) The Rise of Big Tech

Also known as the Tech Giants, Big Tech refers to the largest Information Technology companies. The term most often refers to the Big Five technology companies: Google, Alphabet, Amazon, Apple, Meta and Microsoft. In China, Baidu, Alibaba, Tencent and Xiaomi rival the Big Five.[165]

The term 'Big Tech' became popular around 2017, following the investigation into Russian interference in the 2016 United States elections,

---

[163] Steven Novella, "Demonising 'Big Pharma", *Science-Based Medicine*, 22 April 2010.

[164] "How the Anti-Vax Movement is taking over the Right," *Time*, 06 May 2022.

[165] "We're stuck with the Tech Giants. But They're Stuck with Each Other", *New York Times*, 13 November 2019.

as the role these technology companies played with access to a large amount of user data ("Big Data") and the ability to influence their users came under Congressional review.

iv) Hedge Fund Financial Manipulations

The controversial and often notorious role of huge, independent "hedge funds" has become ubiquitous in the financial markets nowadays. Many view big hedge funds as predatory investors who endanger the financial markets with reckless risk taking. Others view them as unavoidable to balance the markets and a natural means for weeding out the market's internal anomalies.

The "hedge funds", as we know them today, were invented in the 1 980s and the 1990s and referred to a vehicle where people pooled their money to make investments. These funds were privately organized, which ensured that minimum regulation was applicable to such funds. Thus, the fund was mostly free to choose or change its asset classes and investment decisions when required without lengthy processes. Lastly, there was very little restriction on the amount of advantage that could be taken by the fund.

Hedge funds are often notoriously charged with manipulating the stock market by using advanced tactics, often dumping millions of shares of stock at a great price in a short period . By creating mass hysteria and disturbing the markets with their Influence Operations techniques, they are capable of bringing down central banks and national currencies. Thus, George Soros' hedge fund called the "Quantum Fund" is infamous for leading a pack of other hedge funds that nearly bankrupted the British central bank in the 1980s.

The malefic influence of negative hysteria, created by big hedge funds suddenly exiting their positions after making significant profits and on the back of falsely circulated rumours regarding the merits of a stock, hedge funds can bring down financial markets of economies, whose fundamentals might in reality be strong.

Manipulating the stock market can be a lucrative game for hedge funds, where they can move the market up and then fade it, creating a negative feel. The scary thing about this type of market manipulation is that such practices are often legal.

The role of undisclosed election campaign donors, dubious financiers and special interest groups within and outside the country, has also been the subject of regulation and much controversy, ever since Marx's criticism of capitalist democracy.

Chapter VII

Planning and Execution of Influence Operations

Countries have devised various means and models for developing effective Influence Operations (IOs) and built diverse frameworks for integrating them into their larger military campaigns. Today, there are several approaches, methodologies, and tools that assist countries in planning, executing, and in assessing Influence Operations.

Influence Operations are often devised keeping a specified target audience in mind, which may focus on a select elite or members of decision-making group, military formations and personnel, specific population subgroups, or the mass public. Thus, IOs can be devised to focus on a target audience at the individual level, at the group and network level, the adversary's leadership coalition level, or simply at the mass public level. In accordance with the needs of these categories, approaches, models, and tools are identified that help assist in the planning, execution, and assessment of IOs.[166]

IOs Influencing Individuals

In certain instances, countries may seek to influence the attitudes, beliefs, actions, and decisions of specific individuals—for example, of foreign political leaders or high officials to be in sync with the interests of the

---

[166] Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston, "Foundations of Effective Influence Operations: A framework for Enhancing Army Capabilities," Arroyo Centre, RAND Corporation, 2009.

country conducting the IO, or at least not inimical or opposed to them. This requires an in-depth understanding of attitudes and beliefs, and how individuals respond to messages. There is general scholarly agreement that an attitude represents a summary evaluation of a psychological object captured in attribute dimensions, such as good or bad, harmful or beneficial, pleasant or unpleasant.[167]

Research suggests that stronger attitudes remain stable over time and are more resistant to persuasion as well as more predictive of manifest behaviour. There is also evidence linking attitudes to values (favourable valences associated with abstract concepts such as freedom and equality) and ample evidence linking attitudes to subjective norms.[168]

1. Expectancy-Value Model. The most popular conceptualization of attitude—the expectancy-value model of Fishbein, Ajzen, and Feather—suggests that evaluative meaning arises spontaneously and inevitably, as individuals form beliefs about an object. In addition, each belief associates the attitude object with a certain attitude. This approach also provides a theoretical framework for examining resistance to persuasion that focuses on message acceptance, second-order impacts on attitudes not directly addressed in messages, and the evaluation of message attributes.[169]

2. *Elaboration Likelihood Model (ELM).* Petty and Cacioppo's ELM is a dual-process model. It argues that attitudes guide decisions and other behaviours and that there are both central and peripheral routes to persuasion. When individuals are involved in trying to understand an argument and its supporting evidence (i.e., elaboration is high), the central route is more efficacious, as

---

[167] Icek Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behavior*, Prentice Hall, Englewood Cliffs, N.J.,1980.

[168] Roger Tourangeau and Kenneth A. Rasinski, "Cognitive Processes Underlying Context Effects in Attitude Measurement," *Psychological Bulletin*, 103 (3), 1988, pp. 299–314.

[169] M. Fishbein, and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Addison-Wesley, Reading, Mass.,1975.

compared to when individuals are not involved (i.e., elaboration is low), the peripheral route is a more effective approach.[170]

3. *Cognitive Dissonance Theory*. In view of its historical import, scholars note Festinger's cognitive dissonance theory.[171] In its original form, the theory argued that individuals who hold discrepant cognitions are motivated to reduce or eliminate the tension between these cognitions by trying to bring them back into alignment. This can be accomplished, for example, by changing one or more cognitions, adding new cognitions, or altering the relative importance (e.g., discounting) of certain cognitions. Subsequent research has suggested that the concept of cognitive dissonance does not explain dissonant generalized cognitions (e.g., political views), so much as cognitions that challenge one's generally favourable views of oneself: Individuals may be motivated to realign their self-concept or engage in bolstering behaviour when, for example, a freely chosen behaviour results in some foreseeable negative consequence or if dissonance arises from the violation of self-integrity.[172]

4. *The Rationale for Escape from Rationality:* Some areas of study explain changes in attitudes and behaviours that are based on rational cognition and on systematic departures from strict rationality.

5. *Bounded Rationality*: Traditional economic theories of decision-making assumed that man was a rational, utility-maximizing, self-interested actor with perfect information. However, Herbert Simon's theory of bounded rationality argues instead that people are partly rational but that, given the vast complexity of the world and practical constraints on time and other resources for gathering

---

[170] Richard E. Petty and John T. Cacioppo, *Attitudes and Persuasion: Classic and Contemporary Approaches*, Westview Press, Boulder, CO,1996.

[171] Leon Festinger, 'A Theory of Cognitive Dissonance', Stanford University Press, 1957.

[172] E. Aronson, "The Theory of Cognitive Dissonance: A Current Perspective," in L. Berkowitz, (ed.), *Advances in Experimental Social Psychology*, Vol. 4, Academic Press, New York, 1969, pp. 1–34.

> information and making decisions, human rationality is necessarily bounded.[173]

Judgment Under Uncertainty. Again, research by a number of psychologists has aimed to enrich Simon's intuition about bounded rationality by exploring exceptions to strict rationality. Experiments conducted by psychologists Daniel Kahneman, Amos Tversky, and Paul Slovic (1982), for example, have shown that individuals' use of heuristics and biases lead to departures from strict rationality in the form of expected utility calculations, but that many of these departures occur in systematic and predictable ways.[174]

Meanwhile, the theory of reasoned action by Icek Ajsen says that individuals' intentions are the best guides to their behaviour and that their intentions are, in turn, guided by their attitudes toward the behaviour and the subjective norm related to that behaviour. The theory of planned behaviour is an extension of the theory of reasoned action and adds a third variable—perceived behavioural control—as an additional predictor of behaviour.

Although some of the models just described are somewhat general in nature, the poverty of riches created by these competing models suggests the absence of a larger meta-theory or model that integrates and harmonizes these perspectives—and their empirical support— in a coherent and operational way.[175]

This finding is also echoed in J.A.C. Brown's (1963, pp. 103, 148) analysis of propaganda in the First and Second World Wars , which concludes that situational factors were dominant in determining the success or failure of wartime propaganda efforts:

> "Propaganda is successful only when directed at those who are willing to listen, absorb the information, and if possible act on it,

---

[173] Jonathan Bendor, "Herbert A. Simon: Political Scientist," *Annual Review of Political Science*, 6, 2003, pp. 433–471.

[174] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica,* 47 (2), , March 1979, pp. 263–292.

[175] Bertram H. Raven, "Political Applications of the Psychology of Interpersonal Influence and Social Power," *Political Psychology*, 11 (3), 1990, pp. 493–520.

> and this happens only when the other side is in a condition of lowered morale and is already losing the campaign . . . . War propaganda can often change attitudes but, unless the real situation is catastrophic, it rarely changes behaviour; and propaganda which does not lead to action has very largely failed."[176]

Influencing Groups and Networks

The next level from the individual involves influencing the behaviour of individuals in groups and group-level dynamics, decisions, and other behaviours.

The following is meant to provide a brief overview of some of the more important work in these areas:

- *Social Power Theory:* Social psychologist Bertram Raven has focused much of his research on defining and elaborating the concept of "social power". In this model, planners seeking to influence another party assess both their own motivations and those of the target audience, their available power bases, the costs of available influence strategies, and necessary preparations for the influence attempt. In a similar fashion, the target audience also may assess motivations for resisting the attempt to influence and other related factors.[177]

- *Cialdini's Influence Model*: Social psychologist Robert B. Cialdini (2000, 2006) identified what he described as six "weapons of influence": (1) reciprocation, the tendency for people to return a favour; (2) commitment, the tendency for people to honour a commitment; (3) social proof, the tendency for people to behave as they observe others behaving; (4) authority, the tendency to obey authority figures; (5) likeability, i.e., people are more easily persuaded by those whom they like; and (6) scarcity, perceptions of scarcity generate demand. Cialdini also argued for the "foot-

---

[176] J.A.C. Brown, *Techniques of Persuasion: From Propaganda to Brainwashing*, Penguin Books, Baltimore, MD, 1963.

[177] Ibid, pp. 493–520.

in-the-door" phenomenon, which suggests that if small efforts at influence are successful, they can also be used for large efforts.[178]

- *Social Exchange Theory:* The social exchange theory of psychologists J. W. Thibaut and H. H. Kelley (1959) is a general theory of interpersonal relations and group functioning that bases its analysis of social interactions on game theoretic assumptions regarding how people in groups influence each other through the exchange of rewards and costs, and the availability of resources. In this theory of interdependence, individuals try to maximize rewards and minimize costs, and they choose to develop relationships with others based on their assessments of the expected outcome of developing a relationship relative to other possible relationships.[179]

- *Appeals to Fear and Attitude Change*: One of the unique aspects of influence in military operations is the ever-present possibility of coercion through the threat or use of force, and there is some research on the efficacy of appeals to fear in communications. Hovland and his associates (1953), for example, provide some of the earliest theoretical analyses of fear arousal and persuasion. Subsequent work has suggested that low and high levels of fear can interfere with the processing of messages and that moderate levels of fear may lead to the most effective persuasion. Other works have elaborated on Hovland's original formulation and have sought to understand how the severity of a threat, its probability of occurrence, and the availability of coping strategies affect the persuasiveness of communications.[180]

---

[178] Robert B. Cialdiniand David Schroeder, "Increasing Compliance by Legitimizing Paltry Contributions: When Even a Penny Helps," *Journal of Personality and Social Psychology*, 34, October 1976, pp. 599–604.

[179] H. H. Kelley, and J. W. Thibaut, *Interpersonal Relations: A Theory of Interdependence*, John Wiley & Sons, Hoboken, N.J., 1978.

[180] Punam Anand Keller and Lauren GoldbergBlock, "Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration," *Journal of Consumer Research*, 22, March 1996, pp. 448–459.

- *Coercive Persuasion and Thought Reform:* Finally, psychologists Kurt Lewin and Edgar Schein separately considered what may be extreme types of group influence, i.e., coercive persuasion and thought reform ("brainwashing") programmes such as those used by the Chinese on Korean War prisoners. This work suggests that changing attitudes involve three distinct steps: (1) "unfreezing" current attitudes, (2) changing the attitudes, and (3) "refreezing" the new attitudes.

INFLUENCING ADVERSARY LEADERSHIP COALITIONS

Influence Operations can also focus on strategies for influencing adversaries, specifically features that appear to be somewhat distinctive to influence operations against adversary leadership coalitions. Of keen interest to analysts supporting IOs is the question, how either singly or in concert with other policy actions—could these IOs influence an adversary's decision-making, either via direct efforts to persuade specific key leaders or indirectly via efforts to affect factional or coalition manoeuvring that can place additional pressure on adversary leaders.

In this respect, the work of political scientist Alexander L. George constitutes perhaps the most systematic exposition of influence theory in International Relations and security affairs for cases outside the normal lanes of diplomacy, those in which the threat of, or use of, force is present.

Alexander George's research specifically considers the conditions for success or failure for a wide range of available political-military strategies, including:[181]

- Deterrence
- Coercive diplomacy

---

[181] Alexander L. George, "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries," in Barry R. Schneider and Jerrold M. Post, (eds.), *Know Thy Enemy: Profiles of Adversary Leaders and Their Strategic Cultures*, USAF Counterproliferation Center, Maxwell Air Force Base, Alabama, 2002, pp. 271–310.

- Indirect forms of deterrence and coercive diplomacy
- Reassurance
- Conciliation
- Conditional reciprocity
- Graduated reciprocation in tension reduction (GRIT)
- An-eye-for-an-eye strategies
- Behaviour modification strategies or conditional reciprocity
- Dealing with "spoilers" in mediating intrastate conflicts
- Crisis management.

CONCLUSION

In developing any Influence Operation, clarity on the following questions is essential to make the exercise deliver desired outcomes.

a) What are current objectives and how likely are they to be achieved, and if not, what outcomes are most likely under present or plausible conditions?

b) Who are the key target audience, whether an individual, a decision-making group, a military unit, a population subgroup, or the mass population of a nation.

c) Which actors or groups are most influential in political-military outcomes?

d) What strategies (e.g., force or negotiation) are most likely to influence these groups and yield desired outcomes?

e) How much authority/influence do group leaders have over their supporters/followers?

f) What message sources, content, and formats are most likely to be accepted and to foster change?

g) How many messages need to be sent to them? What other actions need to be taken?

Chapter VIII

Counter-Measures

Counter-measures that could be devised against influence measures can be placed into three categories: a) resilience building measures, b) deterrents and c) counter-measures. Resilience measures are generally long-term, aimed to strengthen the State, its institutions and most importantly, society to be able to withstand the impact of IOs. Deterrents are active measures that are devised to disincentivise or incentivise particular behaviour by the adversary. Counter-measures refer to reactive activities designed to respond to actions by the adversary.[182]

Resilience-Building Measures

Methods for promoting resilience in societies against the impact of IOs may include promotion of public awareness about seditious and maligning IOs through education of the general population through media literacy and online hygiene, etc. Professional and credible government communication campaigns could play a key role in this regard. Capacity building could help build resilience, mainly formulating effective legal and regulatory frameworks, involving international agreements and treaties and establishing partnerships with civil society and private sector could prove critical for building the infrastructure to block IO-related malicious activities. In addition, better threat assessment and preparedness for anticipated actions as well as speedy

---

[182] J. Pamment and H. Agardh-Twetman, "Can There Be a Deterrence Strategy for Influence Operations?" *Journal of Information Warfare*, 18 (3), 2019, pp. 123–35, JSTOR athttps://www.jstor.org/stable/26894685 (Accessed 30 June 2023).

communications and response mechanisms of threats could be vital in this respect. Identification and reform of domestic groups, who unwittingly serves foreign interests, the usual "useful idiots" and "fellow travellers" is another resilience-building measure. In case of radicalisation, effective counter-radicalisation programmes (CVE) need to be developed and their scope needs to include other forms of political radicalisation also. In addition, resilience can be built by developing links and ties with adversaries and their societies through diplomacy, business ties, diaspora interactions, student exchanges, and public diplomacy.

DETERRENTS

Deterrents refer to the use of incentives and disincentives towards adversaries in order to deter them from acting in an unfavourable manner. These measures can be called the proverbial carrots and sticks. Among incentives, adversaries can be made less hostile by involving them as part of one's future vision and programme for peace and development, according them respect and friendship and listening to their genuine concerns. The temptation of rewards could be offered to them by granting them access to markets, payments via aid or FDI, technical assistance, etc. They could be made partners in scientific cooperation, in countering terrorism, or people-to-people exchange, etc. Disincentives could be, denial of existing benefits in relations, the threat of imposition of high cost or the raising of existing penalties or costs due to bad behaviour, as well as imposition of new punishments.

COUNTER-MEASURES

Actions taken in reaction to offset the effect of an act is a counter-measure. Precise, measured, and direct countermeasures are generally the most effective. Counter-measures can be both covert and overt, and at times, a non-response could be used as an effective counter-measure.

As part of communication, counter-measures could include denunciation, attribution of the malicious IO to its perpetrator, and discrediting of a narrative. In addition, anticipation and foiling of an act before its completion, takedown of the IO units such as websites or publications, can be used in cases of early detection. Expulsion of

IO agents such as calling out dubious diplomats as 'persona non grata', imposing travel bans on foreign suspects, etc. are other means. Denying adversary capabilities for functioning of societal areas are other measures.

Prosecution, banning and blocking anti-national publications (print and online), counselling, de-radicalisation and rehabilitation measures of reclaimable elements and undertaking conventional and kinetic responses in extreme cases come under counter-measures.[183]

The minimal costs, risks and high level of effectiveness in carrying out peacetime IOs, as a means of winning a war without fighting it, has gained considerable traction in recent years, and both large and small actors recognize their potential, and this form of warfare is likely to grow.

As the intent, effect and objectives of IOs are not just difficult to measure but even observe, the prosecution of State and non-State actors using IOs and CIOs under international law remains a challenging proposition. In such a scenario, there is need for more research and training on the subject not just among security agencies, but also among related civil society elements, to curb the menace of IOs. Research institutions from both the social and technological streams must be involved in studying and countering the growing menace of IOs.

SOME COUNTER-MEASURES FOR INDIA

The Indian strategic community needs to take the growing threat of IOs far more seriously, and the Monograph can only propose a few aspects that require immediate attention in this respect.

1) **Institutional Research and Response**: There is a need for building relevant institutional frameworks to conduct research and to suitably respond to IO threats in real time. Given the hybrid nature of this threat, the importance of civil-military fusion

---

[183] U. Tor, "'Cumulative Deterrence' as a new paradigm for cyber deterrence', *Journal of Strategic Studies*, 40 (1), 2017, pp. 92-117.

involving the Indian military and security agencies, private sector enterprises (particularly from the IT sector), civil society organizations, media organizations, relevant academic institutions, etc. cannot be overstated. If Pakistan established ISPR in the late 1940s, perhaps it is time for the Indian Army to establish its own nodal agency for public relations and narrative dissemination.

2) **Legislative Measures**: The Government needs to introduce legislative reforms for prosecuting foreign perpetrators as well as their Indian aides involved in IO activities. It needs to push international organizations and blocs to set guidelines in this regard and for the prosecution of perpetrators. A more specialised legislative regime to cover IT-related crimes, involving social media-related crimes, deep fakes, false and fake news dissemination, use of crypto currency etc. needs to be in place.

3) **Censorship of OTT, Social Media Content:** In India, OTT content should be subject to censorship and, all major platforms that operate should get their content duly rated by a censor board. The measure is important to not just regulate obscenity, vulgarity and violence, but also anti-national content and drug use from being telecast. Recently, French President Emmanuel Macron blamed social media firms and videogames for catalysing violence in Paris. Freedom of expression cannot serve as a licence for violence and abuse and therefore requires a measure of censorship.

4) **Diaspora Outreach:** India would need to enhance its public diplomacy overseas to counter the negative media campaigns of its adversaries and may have to even reach out to the vast diaspora, especially communities that are targeted by hostile State and non-State actors.

5) **Policy on Madrassa Reform:** A coherent policy on madrassa education, which takes on board the important stakeholders, which is implemented throughout the country, needs to be developed. The policy could look into matters of registration and licencing of madrassas, curriculum building, financing and teachers' training.

When it comes to madrassa reforms, there should be greater efforts towards institutionalising the madrassa system, revamping the

syllabus to include contemporary educational and job requirements, proper auditing of their income, especially the one coming from foreign donors, and introducing greater State regulation of these institutions.

6) **Curtailing China's Ingress in Business, Media and Films**: India should be wary of China's increasing footprint in Indian economic sector, and its growing influence on Indian media and film industries. The use of Chinese advancing AI and deep fake technology has the potential to target vulnerable sections of Indian polity and society and the Government and security agencies must be aware and alert, with appropriate response mechanisms for such eventualities.

7) **Forestalling Exploitation of Political Protests:** Although there has been no evidence of foreign powers meddling in India's electoral processes, the involvement of Khalistani groups based in foreign countries infiltrating the 2020-21 farmers protest should alert intelligence agencies over the growing threats coming from abroad. Therefore, the claims of crowd manipulation and artificially engineered agitational politics, requires a deeper understanding and adequate responsiveness.

8) **R&D in Niche Technologies:** India needs to get ahead of the curve in emerging technological fields (AI, gene technology, extended reality or XR, nanotechnology, etc.) to avert new strategic and societal challenges that may confront her in times ahead. New technological breakthroughs related to psychological and information warfare, such as advanced computing, big data information processing, brain imaging etc., could be critical in the medium to long term.

The threat of IOs is metastasising with new revolutions in the Information and Communications Technology. According to James J.F. Forest,[184] the term Influence Operations needs an upgrade and be recognised as Influence Warfare.

---

[184] James J.F. Forest, *Influence Warfare: How Terrorists and Governments Fight to Shape Perceptions in a War Of Ideas,* Praeger Security International, 2009.

Influence Operations refers to the use of non-military means of psychological, informational and political influence and subversion to undermine the security and governance of a targeted country. Revolutionised by 21st century Information Communication Technology (ICT), Influence Operations (or simply IOs) have today developed into a highly insidious, cost-effective and often non-attributable forms of hybrid warfare.

From Russia's allegedly meddling in the election process of the 2016 US presidential elections to earlier charges of consent manufacturing by the media and crowd manipulation by the US to seed civil strife and colour revolutions to bring about regime change in countries of Eurasia and West Asia, Influence Operations are today even conducted by non-state actors to spread their message of violent extremism or to bring down stock markets through algorithmic trading and issuance of unsubstantiated market reports by hedge fund managers.

This monograph makes in-depth case studies of Influence Operation programmes as reportedly organized and developed by four specific countries — Russia, China, the US and Pakistan, and also studies the way in which non-State actors — like MNCs, NGOs and global terrorist organizations — are increasingly extending their sway.

Dr Adil Rasheed is Research Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) and is Coordinator of the Centre for Counter-Terrorism at the Institute. Author of three noted books: 'Political Islam: Parallel Currents in West Asia and South Asia" (2024), 'Countering the Radical Narrative' (2020) and 'ISIS: Race to Armageddon' (2015), he is one of India's noted scholars in counter-terrorism and hybrid warfare. A student of history and strategic cultures, he writes extensively for Indian and international media groups.

MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

Manohar Parrikar Institute for Defence Studies and Analyses

No.1, Development Enclave, Rao Tula Ram Marg,
Delhi Cantt., New Delhi - 110 010
Tel.: (91-11) 2671-7983 Fax: (91-11) 2615 4191
Website: http://www.idsa.in