STRATEGIC CYBER ENABLED INFORMATION INFLUENCE OPERATIONS (SCEIIO) : NATIONAL ORGANIZATIONAL STRUCTURES FOR INDIA

A Dissertation submitted to the Panjab University, Chandigarh for the award of Master of Philosophy in Social Sciences, in Partial Fulfilment of the Requirement for the Advanced Professional Programme in Public Administration (APPPA)

BY

BRIGADIER MANISH KUMAR MEHTA

Roll No 4613

FACULTY GUIDE : DR. CHARRU MALHOTRA

46th ADVANCED PROFESSIONAL PROGRAMME IN PUBLIC ADMINISTRATION

(2020-21)

INDIAN INSTITUTE OF PUBLIC ADMINISTRATION

NEW DELHI

CERTIFICATE

I have the pleasure to certify that **Brigadier Manish Kumar Mehta** has pursued his research work and prepared the present dissertation titled "**Strategic Cyber Enabled Information Influence Operations (SCEIIO) : National Organizational Structures For India"** under my guidance and supervision. The dissertation is the result of his own research and to the best of my knowledge, no part of it has earlier comprised any other monograph, dissertation or book. This is being submitted to the Panjab University, Chandigarh, for the purpose of Master of Philosophy in Social Sciences in Partial fulfilment of the requirement for the Advanced Professional Programme in Public Administration of Indian Institute of Public Administration (IIPA), New Delhi.

I recommend that the dissertation of **Brigadier Manish Kumar Mehta** is worthy of consideration for the award of M.Phil degree of Panjab University, Chandigarh.

(Dr Charru Malhotra)

Indian Institute of Public Administration

I.P. Estate, Ring Road,

New Delhi-110002

Acknowledgement

Foremost, I would like to express my sincere gratitude to my guide Dr. Charru Malhotra for the consistent support, generous guidance, patience, motivation, enthusiasm, and her immense knowledge for conducting this study in a very short period of time. Her guidance helped me during the research and writing of this dissertation. She also, consistently, encouraged me by referring to me relevant and interesting information for my dissertation. I could not have imagined having a better guide and mentor for my M. Phil dissertation.

I would also like to thank the DG, IIPA for giving me this opportunity to choose a very relevant subject and providing the much needed guidance at the proposal stage and infrastructural facilities to complete the work. I want to thank the IIPA library staff for the kind cooperation and making the required books available. I am grateful to all the experts and Dr Roma Mitra for giving very valuable comments during the research proposal presentations which have helped me a lot in conducting this research work. I would like to thank the Course Coordinator of 46th APPPA, Dr. Charru Malhotra, also my Guide, for creating a very conducive and pleasant environment throughout the course, and also showing a very considerate attitude regarding timelines of various assignments especially the dissertation work. I would also to thank the APPPA office staff for providing excellent support.

I would fail in my duty if I do not thank the Department of Personnel & Training (DoP&T), the Government of India, for providing this wonderful opportunity to join the 46th APPPA course thus widening vistas of my knowledge and meeting the wonderful and bright officers from various streams of Indian Civil Services.

Table of Contents

EXECUTIVE SUMMARY

1. Exponential and continuously ongoing expansion of global cyberspace has catapulted the Information Environment into an unprecedented pole position where it can be a prime driver for Comprehensive National Power (CNP). The ability to dominate this domain both in terms of protection and influence based manoeuvre will strengthen nations deeply. Disinformation, Misinformation, Propaganda and Fake News have been weaponized to influence adversary nations both during peace and war at scales unimaginable just a decade ago. Also, shift and convergence of Information Warfare domains like Psychological Warfare and Media Warfare into cyberspace has resulted in the terms 'Cyber' and 'Information' being used interchangeably more often than not. Hence, both authoritarian states and liberal democracies have or are in the process of creating organizational structures to effectively carry out Strategic Cyber Enabled Information Influence Operations (SCEIIO), both for countering disinformation and prosecuting influence operations.

2. The dissertation seeks to arrive at a configuration of organizational structures for India for conduct of SCEIIO. In so doing, it traverses the following waypoints:-

(a) There was a need to arrive at and de-clutter the lexicon connected to Information Operations/Information Warfare and the terminology-path underpinning the adoption of the term SCEIIO. After delving into the background of various synonymous terms especially based on the US DoD publications and certain other scholarly works, Cyber Enabled Influence Operations have been bifurcated into Cyber Enabled Technical Influence Operations (CETIO) and Cyber Enabled Information Influence Operations(CEIIO). CEIIO target the Cognitive Dimension of the Information

environment and when done at the national level to support national security objectives they are termed as Strategic CEIIO (SCEIIO).

(b) Thereafter, an effort has been made to understand global trends in SCEIIO more commonly termed as Disinformation. A comparison between the US and Russian SCEIIO brings out important lessons connected to how democracies and authoritarian states view and conduct these operations differently. SCEIIO would mostly be conducted across the entire peace-war continuum. Therefore, the nature and types of operations carried out during various phases have been studied. Since, election interference is a major area of concern, analysis of such interference by certain states clearly brings out the need for democracies to focus on protecting this core function of democratic process.

(c) The organizational structures of major global players like the USA, Russia, China and European Union bring forth the varied range of departments /agencies/organizations involved in this effort and the need to synergise their efforts. It also emerges, fairly clearly, that authoritarian states have a more centralized control and execution model with the execution agencies spread across a wide spectrum of intelligence, military and non-state actors to avoid attribution. They also see SCEIIO as a seamless continuum of operations in Peace and War. Democracies like the USA have struggled as SCEIIO was more of a military construct in the form of support operations for conventional conflicts. The adaptation from defending against such operations through various fragmented organizations in various ministries and ensuring that suitable organizational changes are effected to prosecute such operations in a focused and synergised manner with adequate oversight is a work in progress.

(d) The recommended structure for India for conduct of SCEIIO is centred around a Defence-Civil mix with control and oversight by the existing National Information Board (NIB) housed within the NSCS. Based on varied inputs from the preceding analysis and ground realities, it has also emerged that ideally Defence Forces should be the lead agency within the organizational structure for SCEIIO. Accordingly, two major recommendations are ; creation of a National Information Operations Agency(NIOA) within the NSCS and upscaling of the existing Defence Cyber Agency(DCyA) into Defence Information Operations Command (DIOC). An interagency type structure has been recommended with various ministries and intelligence agencies feeding into the NIOA-DIOC combine under the NIB. It has also been recommended that the NIOA and DIOC be dual hatted by a serving Three-Star from Defence Forces to provide the necessary unity in command and purpose.

3. India's democratic and diverse socio-political landscape and an exponentially expanding social media presence offers our adversaries a potent attack surface for prosecuting SCEIIO. It is important that we develop capacities and are structurally organized not just to defend but to be able to deter through prosecution of SCEIIO against our adversaries. The dissertation has offered one such model.

CHAPTER I : INTRODUCTION

" It sounds a dreadful thing to say, but there are things that don't necessarily need to be true as long as they are Believed."

– Alexander Nix

" People cannot see Influence Operations. You need to tell them about it"

– Latvian Official

1. Internet is the single most disruptive force that threatens the concept of the Westphalian Nation-State. Social Media which rides on the internet and is transnational in nature, is intrinsically in conflict with the power and exclusivity of geographic delimitation that characterizes a nation-state. Hence, it is only natural for nation-states to react to the challenges posed by social media. Social media has empowered citizens and individuals and has dismantled traditional information and media hierarchies. The 20th century nation state's traditional primacy over use of force and control of information have been diluted by non state actors/terrorism and social media platforms, respectively. Power has moved from hierarchies to citizens and networks. Social media shatters unity and divides people in two ways – first, it puts them at loggerheads, second, it puts them in silos which is more insidious as they live in echo chambers of disinformation where they can be easily influenced.

2. Influence is a commonly used form, mechanism, and instrument of power that is, according to Robert Dhal (1957), the ability for "A to have B doing, to the extent that he can get B to do, something that B would not otherwise do". Brangetto &

Veenendaal (2016), expanded on this definition by noting that the objective of influence is thus to exert power by shaping the behaviour and opinions of a target audience through the dissemination of information and conveying of messages. Throughout history, national governments and sub-national entities have resorted to using information and influence operations to advance their national and international interests, whether they were of a security, economic or political order (Matteo Bonfanti, 2019). One can find a plethora of examples of such activities, whether in peacetime, within the context of rivalry, political or economic tensions or during open conflict or warfare. Although influence operations are often regarded as modern inventions, examples can be found throughout human history. In the 12th century AD, Genghis Khan and his tribesmen orchestrated one of the first large-scale disinformation campaigns by widely disseminating rumours about the horde's strength and cruelty to weaken an enemy's resistance.

3. Similarly, during World War I, allied airplanes dropped leaflets behind the German lines of defence to erode troop morale and call upon them to surrender. Similar influence operations were also conducted during World War II, the Cold War, the two wars in Iraq, and more recently in Libya, Afghanistan and Syria (Bonfanti, 2019). During the Cold War, propaganda in all its various forms was the primary tool for pushing ideological narratives into foreign spheres of influence. Such attempts to undermine or change information narratives have continued over the past years, notably in 2016 and 2017, with allegations of Russian interference in Latvian news media and the Indonesian government accusing "terrorists" of releasing fake anti-government news reports.

Definition Maze : Influence Operations / Activities and Techniques

4. While literature on the subject of information operations has grown exponentially in recent years, there is a fundamental "lack of consensus when it comes to defining all the elements that make up the strategic application of power in the information domain" (Brangetto & Veenendaal, 2016). Specifically, a number of similar terms have emerged throughout contemporary history that are still extensively used in the literature to describe influence activities. Examples range from propaganda, political warfare, psychological warfare, and information warfare to psychological operations, information operations, neocortical warfare, perception management, and netwar. These various terms are supported by specific context-dependent case studies conducted over time. It therefore seems relevant to review some of the most important terms in chronological order, starting with propaganda:-

5. **Propaganda**. The origins of the term "propaganda" can be traced back to the *Congregatio de Propaganda Fide*, a 17th-century Catholic committee that fought the Reformation (Walton, 1997). It promoted and advocated for the church's doctrine and viewpoints though various means, including printed pamphlets, seminars and missionaries. More recently, the widespread use of the term by Allied Forces during the two World Wars and the Cold War to refer specifically to hostile opinion-forming activities has strongly entrenched its present negative connotation in popular minds. Indeed, today it is commonly used in both times of peace and war to attack a rival's arguments on the basis that they are unsound, intentionally deceptive, unethical, illogical and aimed at manipulating a mass audience. Within the US military literature, the term "propaganda" has been used to denote lies and distortions normally associated with an enemy and has been differentiated from perception management.

6. **Political Warfare**. The term and concept of *political warfare* has been in use since World War I and was originally coined by the UK (Schleifer, 2014). Its application, however, dates back several decades, if not centuries. According to Blank (2017), political warfare can be regarded as the logical application of Clausewitz's doctrine in times of peace. Specifically, he defines it as "the employment of all the means at a nation's command, short of war, to achieve its national objectives, both in an overt and covert fashion." Relevant activities range from peaceful to aggressive means as well as from overt actions (e.g. political alliances, economic measures, or white propaganda) to covert operations (e.g. support of foreign resistance cells or black propaganda) (Blank, 2017).

7. **Psychological Warfare And Operations**. The concept of *psychological warfare* (PSYWAR) was officially developed by the US forces when they joined World War II (Schleifer, 2014) but actors have engaged in it since ancient times. Specifically, the term "denotes any action which is practiced mainly by psychological methods with the aim of evoking a planned psychological reaction in other people". Similar to political warfare, it makes use of various techniques to influence a target audience's values, beliefs, emotions, motives, rationales, or behaviours to reinforce behaviours favourable to the user's objectives. For example, it can be used to strengthen the resolve of allies or resistance fighters as well as to undermine and erode the morale and psychological state of enemy troops. There are a number of historical examples of specialized units trained for this kind of warfare, notably during World War II by the German and Allied Forces but also by the US Armed Forces during the Korean and Vietnam wars. Accordingly, PSYWAR closely relates to the use of psychological operations (PSYOPs), a term that rose to pre-eminence after the end of the Korean War and is still in use today as part of the US understanding of

information warfare capabilities (Schleifer, 2014). PSYOPs are all about using information dissemination to cripple the target's morale and will to resist. Classical PSYOP techniques include the air-dropping of propaganda leaflets and use of airborne loudspeakers to broadcast demands for surrender. The underlying rationale thus lies in persuasion through the use of different logics (i.e. fear, desire or ideology) to promote specific emotions, attitudes and behaviours. As such, PSYOPs can be used in times of peace or open war and are considered a force multiplier using nonviolent means in often violent environments. Furthermore, PSYOPs are sometimes divided into three levels (i.e. strategic, operational and tactical) by practitioners to reflect the areas in and the times at which they are expected to be deployed. Each level has its own goal (e.g. to promote a positive image, to deter, encourage, recruit, or lower morale), context, and means of delivery. In the past, the primary means of delivery were newspapers, paper leaflets, and the airwaves (radio and television). Today, soldiers have access via cellular phones to television, e-mails, and social media, as well as old and new media (Schleifer, 2014).

8. **Information Warfare (IW)**. Another preeminent, but contentious, concept in use since the 80s – mostly in the US military and the intelligence community – is that of IW, which is motivated by opportunities and that arise from the dependence of individuals and societies on vulnerable ICT and systems. The term has become an umbrella term for conceptually understanding cyberwar, hackerwar, netwar, virtual war, and other network-centric conflicts. It refers to the use of "a range of measures or actions (including information & ICT) intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary". Specifically, IW may include a wide variety of activities, which are closely linked to psychological warfare and

include (Kiyuna & Conyers, 2015): collecting tactical information; ensuring that one's own information is valid; spreading propaganda or disinformation to demoralize or manipulate the enemy and the public; undermining the quality of opposing forces' information; and denying information-collection opportunities to opposing forces. Several scholars have extensively written and theorized about IW, notably Schwartau and Libicki, who have both developed different classifications and forms of IW. According to Schwartau, IW can be broken down into three sub-groups, namely personal, corporate and global information warfare (Schwartau, 1994), with the scale and risks increasing between one category and the next. Meanwhile, according to Libicki, IW occurs in seven different forms (Libicki, 1995): command and control warfare; intelligence warfare; electronic warfare; psychological warfare; hacker warfare; economic-information warfare; and cyber warfare. Over the years, other scholars have, however, divided IW into two main strands, both of which are based on earlier concepts, namely "soft IW", which includes psychological warfare, media warfare and perception management; and "hard IW", which includes net/electronic warfare. In any event, IW transcends the traditional domains of warfare and finds itself at the intersection of the information, physical and cognitive/social domains. Its scope goes beyond the military and touches on the political, diplomatic and economic spheres of information. Furthermore, the action of IW is defined as information operations (IOs) in the US military literature, a term that has been widely adopted by other actors. As such, IOs are formally (and quite broadly) defined by the US DoD in JP 3-13 as "actions taken in times of crisis or conflict to affect adversary information and information systems while defending one's own information and information systems" (Joint Chiefs of Staff, 2014). Accordingly, IOs traditionally comprise five core capabilities viz. Computer Network Operations (CNO) (which comprised of

Computer Network Attack (CNA), Computer Network Defense (CND) and Computer Network Exploitation (CNE)), Psychological Operations (PSYOP), Electronic Warfare (EW), Operations Security (OPSEC) and Military Deception (MILDEC). In addition, these core capabilities are accompanied by related and supporting activities, which are public diplomacy (PD), public affairs (PA), civil military operations, information assurance, physical security, physical attack, and counter intelligence. As a note, the term computer network operations (CNOs) has been replaced in the more recent literature by cyberspace operations (COs), which the US DoD (Joint Chiefs of Staff, 2018) broadly defines as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace". As such, CO missions can be offensive (OCO), defensive (DCO) and DODIN operations (relating to the ministries' internal networks). In terms of actions, these encompass cyberspace security, cyberspace defense, cyberspace exploitation, and cyberspace attacks. The latter three replace the (still widely used) terms of CNA, CND and CNE. In terms of techniques, these involve the use of computer technology and cyber weapons to shut down, degrade, corrupt, or destroy various information systems. **This understanding and classification of IW and IOs are, however, neither universal nor do they represent a uniform Western vision**. Indeed, many other states, from France to the United Kingdom, have developed their own understandings and doctrines. Another particular case is none other than Russia, which has a long tradition of strategic thinking about the role of information in projecting national power, the best-known examples of which include the active measures the country took during the Cold War. In contrast to the US view, Russia's understanding of IW, or information confrontation (informatsionoye protivoborstvo [IP]), does not distinguish between war and peace activities. According to Pernik (2018), "borders between internal and

external, tactical, operational and strategic levels of operations, and forms of warfare (offense and defence) and of coercion are heavily blurred". This mostly goes back to the country's national security policy, which is built upon the perception that Russia is under constant siege by foreign influence and thus finds itself in a constant struggle for its survival (Blank, 2017). Furthermore, the Russian approach to IW is much more holistic and whole-of-government. It mobilizes the entire Russian state (and para-state) apparatus for a wide variety of activities, which include "intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems, and propaganda" (Brangetto & Veenendaal, 2016). As such, most of the Russian information warfare activities are fundamentally non-military (or at least less military than their US counterparts).

9. **Influence Operations**. Among the IO capabilities described above, four main objectives can be identified, which are : to influence/inform; to deceive; to deny/protect; and to exploit/attack. Following these lines, IOs can be divided into two broad strands. The first is Technical Influence Operations *(TIOs)*, which target the logical layers of the information space and include information delivery systems, data servers and network nodes. This strand thus includes operations such as EW, OPSEC, OCO, or DCO. The second is Information Influence Operations *(IIOs)* (information influence activities or cognitive influence activities), which are focused on the social and psychological aspects of information operations and aim to affect the will, behaviour and morale of adversaries. This strand includes elements out of the military playbook such as PSYOPS and MILDEC but also public affairs and military-civilian relations. IIOs can in turn be considered as a subset of Influence Operations but may

be limited to military operations in times of armed conflict. Influence operations are, however, not limited to the military context, but form part of a larger effort by nations to exert power over adversaries in multiple spheres (i.e. military, diplomatic, economic). These efforts can, for example, involve targeted corruption; funding and setting up Potemkin villages (e.g. political parties, think thanks or academic institutions); putting in place coercive economic means; or exploiting ethnic, linguistic, regional, religious, and social tensions in society (Pamment et al., 2018**). Influence operations are therefore an umbrella term covering all operations in the information domain, including all soft power activities (e.g. public diplomacy) intended to galvanize a target audience (e.g. individuals, specific groups, or a broad audience) to accept approaches and to adopt decisions that mesh with the interests of the instigators of the operation (Cohen & Bar'el, 2017). Specifically, they can be defined as:**

> **"the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict aimed at influencing decisions, perceptions and behaviour of political leaders, the population or particular target groups (such as experts, military personnel or the media) with the objective of achieving the state actor's security policy objectives".**

According to Pamment et al. (2018), influence operations are underpinned by a number of core elements. On the one hand, with the exception of public diplomacy, they are – at least in the context of peace – regarded as illegitimate attempts to influence opinion-formation and the behaviour of targets (domestically or abroad). This is because they are inherently deceptive with the intention to do harm and

disrupt. As such, they constitute interference with normal behaviour and opinion formation, but also domestic (democratic) processes and the sovereignty of states. Adding to that, influence operations exploit different sets of existing societal and individual vulnerabilities in opinion formation and the epistemic chain linked to our media system as well as our public opinion and cognitive processes. Furthermore, influence operations are conducted with the intention to benefit and advance the strategic interests of their sponsor, whether this is a state, a non-state or a proxy group. They are conducted in a wide spectrum of settings, which includes the contexts of peace and war but also ambiguous contexts such as hybrid and asymmetric conflicts.

10. **Types of Information- Influence Operations**. In common parlance, the term "disinformation campaign" is often used interchangeably with information operations. However, disinformation or deception is only one of the informational tools that can be exploited as part of an IO strategy; factual information can also be used to achieve strategic goals and in some cases more effectively than deceptive means. Different categories of information may be used in IO, including the following:-

(a) **Misinformation**. This is the spreading of unintentionally false information. Examples include internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. Misinformation can have the effect of sowing divisiveness and chaos in a target society, as the truth becomes harder to discern.

(b) **Disinformation**. Unlike misinformation, disinformation is intentionally false. Examples include planting deliberately false news stories in

the media, manufacturing protests, doctoring pictures, and tampering with private and/or classified communications before their widespread release.

(c) **Fake News**. Purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information that mimics the form of mainstream news.

Information Environment

11. All instruments of national power—diplomatic, informational, military, and economic (DIME)—can be projected and employed in the information environment. To bring the term SCEIIO into perspective it is important that the construct of Information Operations and Influence Operations is understood. US DoD manual JP 3-13 defines the Information Environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive (**Figure 1.1**).

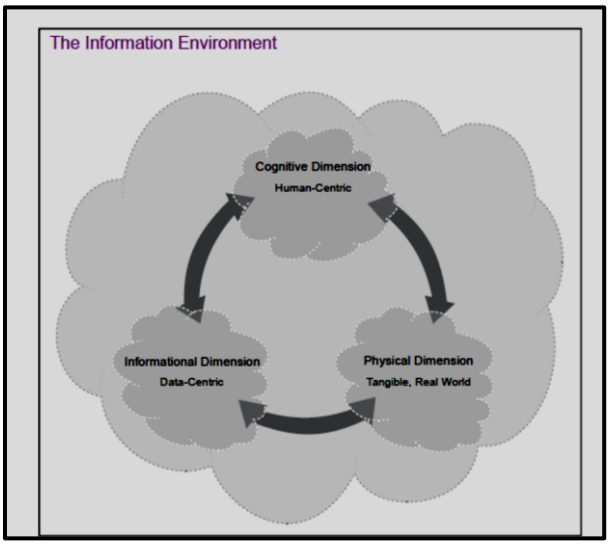


Figure 1.1 – The Information Environment

(a) **The Physical Dimension.** The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a diffused network connected across national, economic, and geographical boundaries.

(b) **The Informational Dimension.** The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.

(c) **The Cognitive Dimension.** The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is

critical for understanding how to best influence the mind of the decision maker and create the desired effects. As such, this dimension constitutes the most important component of the information environment.

12. Information Operations largely target the Cognitive Dimension but as support operations may also address the Physical and Informational Dimensions. One formulation which also interchangeably de-components Information Warfare is given below in **Figure 1.2**.The term Psychological Warfare here could be replaced by a more umbrella term like Influence Operations or Cognitive Dimension Operations.

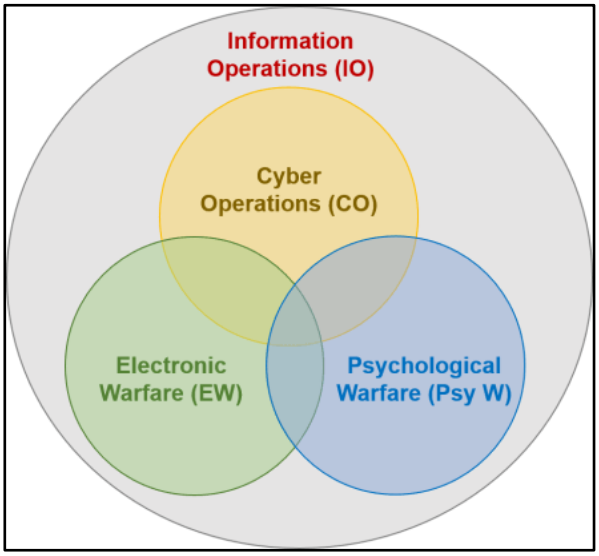


Figure 1.2 – Components of Information Operations

13. The instruments of national power (diplomatic, informational, military, and economic) provide leaders with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in

the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. As the strategic environment continues to change, so does information operations (IO). Based on these changes, **the Secretary of Defense, US DoD, now characterizes IO as the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.**

14. Hence Information – Influence Operations which address the Cognitive Dimension could have the subsets as shown in **Figure 1.3**. This is largely aligned to the US DoD JP 3-13.

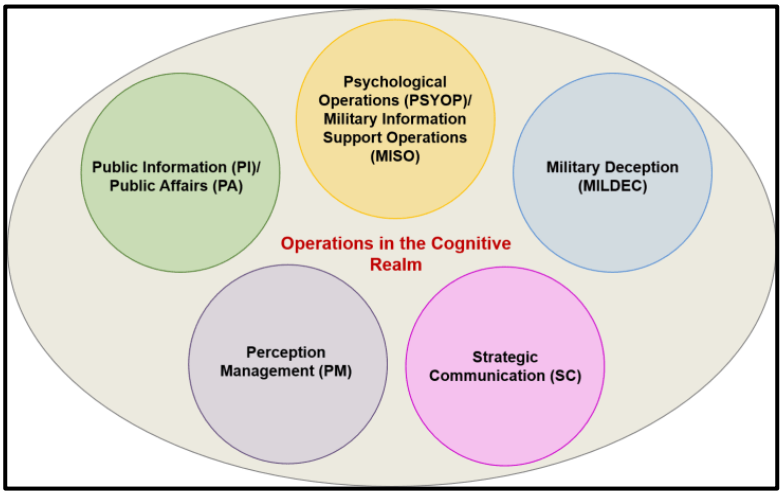


Figure 1.3 – Subsets of Information Influence Operations

15. Indian Armed Forces have so far not made any distinction between the technical and influence aspects of IO. Importantly, India's Joint Doctrine for Perception Management (PM) and Psychological Operations (Psy Ops) considers IO and Psy Ops as sub-disciplines of PM, which is conceptualized as encompassing all information and cognitive operations.

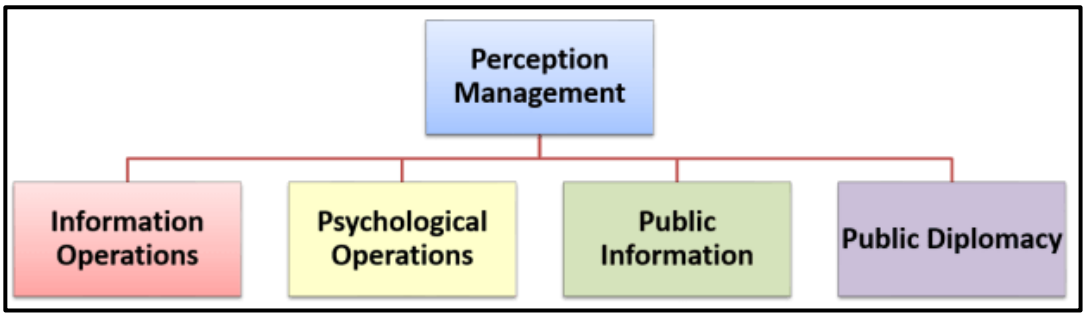


Figure 1.3 A – India's Joint Doctrine for Perception Management (PM) and Psychological Operations (Psy Ops)

16. The Indian Army IW doctrine, which considers CO, EW and Psy W as the three primary components of IW, also does not treat technical and cognitive facets of IO differently. Lt Gen RS Panwar (Retd), in a series on *IW Structures for the Indian Armed Forces*, argues that Indian doctrines should classify various functions of IO into the following two streams: *Information-Technical Operations (ITO)* and *Information-Psychological Operations (IPO)*, with various IO functions clubbed under each as depicted below:-

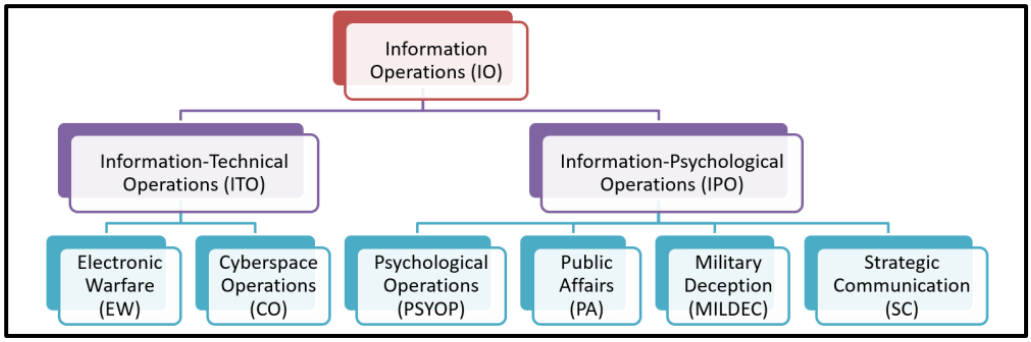


Figure 1.3 B – Classification of Information Operations

Information Operations in Cyberspace

17. William Gibson coined the term cyberspace in his 1984 novel, *Neuromancer*, as a "consensual hallucination experienced daily by billions of legitimate operators, in

every nation, by children being taught mathematical concepts.... A graphic representation of data abstracted from the banks of every computer in the human system." This definition emphasizes the human element, with cyberspace as something that exists in people's minds.

18. In JP 3-12, DOD defines cyberspace as "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Some have criticized this as lacking the cognitive, human element that the internet represents, which in turn could adversely affect how the military organizes, trains, and equips for IO.

19. Cyberspace presents a force multiplier for IW activities. Social media and botnets can amplify a message or narrative, using all three elements of information to foment discord and confusion in a target audience. Much of today's IW is conducted in cyberspace, leading many to associate IO with cyber security. Within DOD, however, IO and Cyberspace Operations are distinct doctrinal activities. Cyberspace operations can be used to achieve strategic information warfare goals; an offensive cyberattack, for example, may be used to create psychological effects in a target population. A foreign country may use cyberattacks to influence decision making and change behaviours, for example the Democratic People's Republic of Korea (DPRK)-attributed cyberattacks on Sony in late 2014. Cyber operations may be conducted for other purposes, such as to disable or deny access to an adversary's lines of communication, or to degrade components of critical infrastructure that may be used for nefarious purposes.

20. IO may be overt, such as a government's production and dissemination of materials intended to convey democratic values. In this case, the government sponsorship of such activity is known. Covert operations are those in which government sponsorship is denied if exposed. The anonymity afforded by cyberspace can present an ideal battle space to conduct covert information operations. In addition, IO may take place outside of cyberspace.

21. Although several official documents now refer to "information warfare" in other countries, the United States has no formal government definition of IW. The DOD definition of information operations refers only to military operations and does not emphasize the use of cyberspace to achieve non-military strategic objectives. Similarly, there is no commonly accepted definition of "cyberwarfare" ; rather, the military refers to offensive and defensive cyberspace operations, with cyberspace as a warfighting domain or operating environment.

22. Cyberspace operations differ from information operations, which are specifically concerned with the use of information-related capabilities, such as military information support operations or military deception. **Cyber-enabled information operations can be characterized as IO conducted in cyberspace**. Just as IO carries its own doctrine and associated organizational structures, so do cyberspace operations, which are generally considered the purview of e.g. the United States Cyber Command or the Chinese PLA SSF.

Cyber Enabled Influence Operations

23. Influence and influence operations have been exercised since times immemorial by all kinds of actors, whether individuals, groups, or states, and in all kind of forms. States in particular have been using them to further their strategic interests in

various contexts, whether during wars, peace or the large spectrum in between. Today, however, the dawn of the information age has seen these influence activities migrate toward cyberspace, making use of the opportunities that new ICT, most notably social media, has to offer. Targets, end-objectives and strategies of CIOs are the same as with traditional influence operations. However, they differ in that they involve new digital tools (e.g. cyberattacks, bots or social media), which have greatly enhanced psychological warfare techniques and strategies. In this regard, a distinction can be made between **two types of CIOs**: ***cyber-enabled technical influence operations*** **(CETIOs) and** ***cyber-enabled Information influence operations*** **(CEIIOs)**, with the former relying on a repertoire of cyber capabilities with varying degrees of sophistication to influence targets and the latter focusing on utilizing cyberspace to shape public opinion and decision-making processes through the use of social bots, dark ads, memes and the spread of disinformation. These will be discussed later. Cyberspace has acted as an equalizer and enabler for influence operations. Notably, the relatively low cost of entry, widespread availability of tools and possibility to circumvent traditional controls of information have allowed anyone to engage in CIOs. Meanwhile, the ease, speed and virality of information dissemination as well as the increasing reach, scale, penetration, precision and personalization of information targeting have greatly enabled their use. These elements, and the fact that CIOs present an asymmetric option and tool for counterbalancing conventional power at little cost yet with great flexibility, with low risks of detection and escalation but high potential results, has made them particularly attractive for state and non-state actors alike. However, due to the complexity of observing and measuring intent and effect, the medium to long-term strategic implications and impacts of these types of operations are still uncertain.

Cyber Enabled Influence Operations : Types

24. The advent of the information age, with its innovative technologies (including the internet) and socio-economic-cultural changes, has progressively transformed the information environment both in its constituent elements and its inherent dynamics, which contributed to the formation of the additional dimension that is cyberspace: a

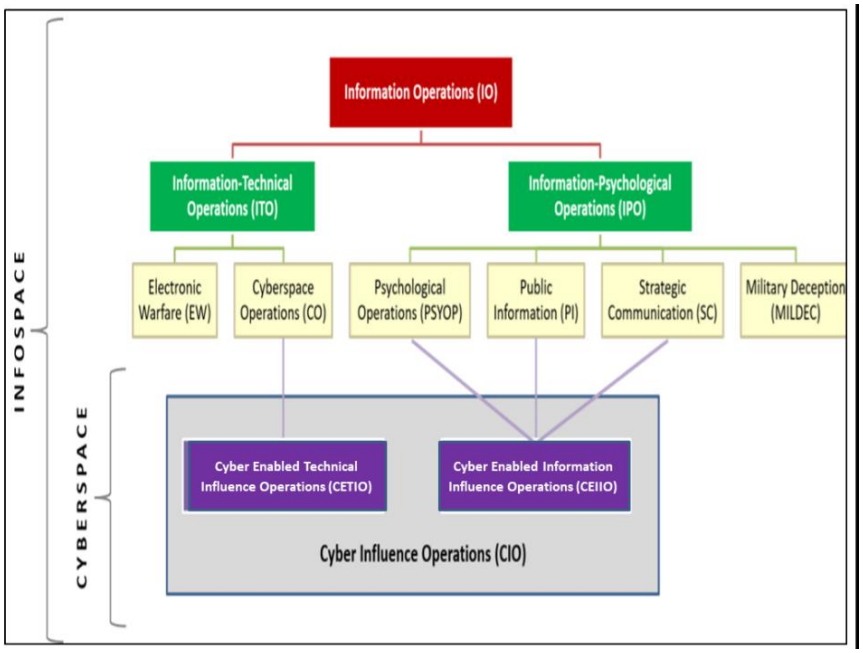


Figure 1.3 B – Classification of Cyber Enabled Influence Operations

space within which a wide range of actors have access to and the ability to use information for a myriad of activities, including influence-related ones. This is especially true nowadays, as one consequence of this transformation has been that the control and release of information is no longer monopolized by only a few actors (i.e. the state and accredited media). Indeed, today, any organization or individual can create and disseminate information to a mass audience using internet-connected devices and social media (Bonfanti, 2019). An additional consequence has been the financial reconfiguration of large parts of the media system (i.e. social media, online media), which has prioritized commercial imperatives over the reliability and integrity

of information. One common example is the use of misleading information or disinformation for clickbait and advertising revenue. Accordingly, many traditional influence activities (e.g. propaganda) have increasingly shifted to cyberspace. In the literature, this has notably led to the emergence of a plethora of related terms to denote this particular vector. These include "cyber-propaganda", "cyber-enhanced disinformation campaigns", "cyber-abetted inference", "cyber-persuasion activities", "influence cyber operations", "cyber hybrid operations" and "cyber-enabled information operations", among others. However, these terms are often given and used without a clear definition. In addition, they also tend to not distinguish between influence campaigns that may be executed fully or partially in and through cyberspace on the one hand, and cyberattacks that apply cyber capabilities with the purpose of causing certain effects in cyberspace on the other (Pernik, 2018). **This term *cyber enabled influence operations* (CEIOs) refers to activities that are run in cyber-space, leverage the distributed vulnerabilities of cyberspace, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes** (Bonfanti, 2019).

25. As mentioned earlier, what has changed between Influence operations then and cyber influence operations now are the tools and techniques used. In order to further examine these, one must first make an additional distinction between two categories of CEIOs, namely Cyber-Enabled Technical Influence Operations (CETIOs); and Cyber-Enabled Information Influence Operations (CEIIOs). This distinction is also important in terms of counter and protection measures. For instance, better social media content filters and regulations, greater media literacy, or improved

educational programs could counter the impact and spread of disinformation. In contrast, cyberattacks and their detection require the development of highly specialized technical and contextual (e.g. culture, language) expertise as well as certain investments (Pernik, 2018). In addition, the choice of response to such cyber influence activities will also depend on the legality or illegality of relevant acts, an element which differs between the two.

26. **Cyber-Enabled Technical Influence Operations (CETIOs)** CETIOs are a subset of cyber enabled influence operations that are often referred to as cyberattacks in support of influence operations or influence cyber operations (ICOs). Specifically, they affect the logical layer of cyberspace through intrusive means 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 (Brangetto & Veenendaal, 2016). The spectrum of CETIOs ranges from low to high-end attacks (Pernik, 2018). As a note, their attribution can be affected by false-flag attacks, where the use of specific techniques (IP spoofing, fake lines of code in a specific language) results in misattribution. At their lowest end, CETIOs are aimed at sowing confusion, disseminating propaganda, undermining credibility and trust, or disrupting activities. They are used across the spectrum of peacetime and war (including in low-intensity conflict). Typically, PII harvesting for future exploitation by targeted CEIIO is also CETIO. A recent example of an alleged cyber attack on the Indian electric grids while negotiations were on to resolve the LAC crisis with China is a classic CEITO wherein an effort was possibly made to influence Indian decision makers.(David Sanger & Emily Schmall , 2021). Similarly, as exposed by Cyfirma a cyber intelligence firm in Singapore, cyberattacks on the IT

systems of world's' largest Vaccine producer Serum Institute Of India as well as Bharat Biotech was again a CEITO to diminish India's stature and influence our decision makers, a "Winning without Fighting" Sun Tzu imprint.

27. **Cyber-Enabled Information Influence Operations (CEIIOs)**. Cyber-Enabled Information Influence Operations (CEIIOs) differ from the previous category in that they do not involve the deployment of cyber capabilities to affect either the physical or logical layer of cyberspace. Instead, they target and attack the semantic layer of cyberspace (i.e. information content) through a wide variety of tools and techniques in order to support and amplify various political, diplomatic, economic, and military pressures. As such, they constitute non-coercive or "soft" influence operations. Most of these techniques (e.g. big data exploitation or the purchase of political ads) are not illegal per se but often fall into a grey area of legality, frequently due to the absence of relevant domestic or international legal frameworks and diverging national understandings. The alleged Russian interference through Facebook in American elections in 2016 and the Cambridge Analytica operations during Brexit are examples.

28. **Integrated Employment of CETIO and CEIIO Capabilities** In certain types of CIO, a combination of CETIO and CEIIO may be resorted to for achieving the desired effects. For instance, a particular set of individuals may be targeted with suitably crafted messages on social platforms based on their psychographic profiles. In order to do this, CETIO may be employed to first obtain their profiles/PII using intrusive CO (eg, by hacking the database of social networking websites), followed by targeted messaging using CEIIO expertise. The Cambridge Analytica data breach and

the follow-up tailored advertisements in the Ted Cruz campaign is an example of an integrated employment of CETIO and CEIIO. In certain other cases this may be well spaced in time wherein acquiring PII data through CETIO and executing multiple CEIIOs could be a possibility. A diagrammatic representation (Lt Gen RS Panwar (Retd)) below, modified marginally, contextualises these various categories.

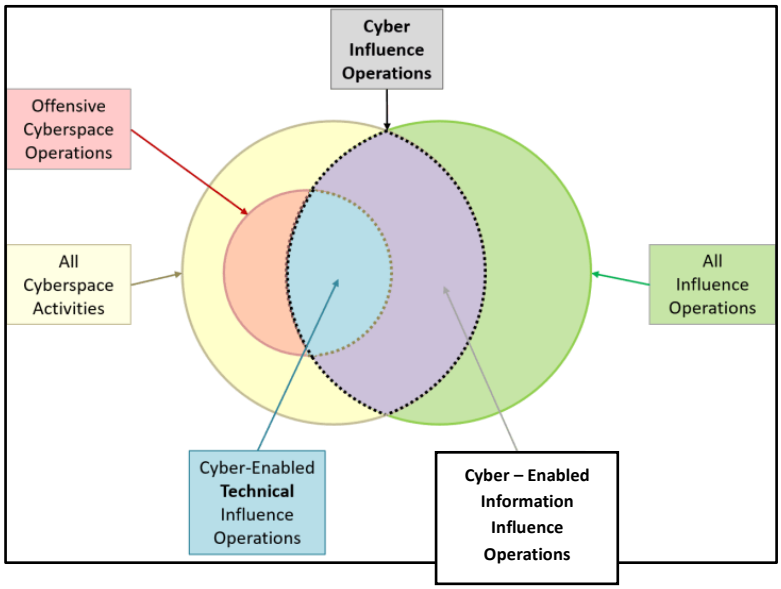


Figure 1.4 – Cyber Enabled Influence Operations

29. **<u>Strategic CEIIO (SCEIIO)</u>**. With CIO being an active part of military operations at all levels as well as Nation- State operations across the entire continuum of conflict, it is important that the standard classifications of Strategic, Operational and Tactical are applied to CEIIO. Defence forces, as part of their operational planning will configure and plan CEIIO in support of their Kinetic or Contact Operations. These, in most cases, would be at the Operational and Tactical level. Strategic level CEIIO would have to be a continuous process to undermine our adversaries and address weaknesses/voids in their strategic orientation and national vulnerabilities/faultlines. They would require a whole- of –government approach and

be planned and executed to support achievement of national security objectives at the highest level. Countering adversary SCEIIO would also be a key component of own SCEIIO. This dissertation addresses the need for organizational structures at the National level for conduct of SCEIIO.

30. **Use of Interchangable Terms**. While the term SCEIIO has been derived to specifically refer to such operations, online literature and articles interchangeably use terms such as Disinformation, Influence Operations, Information Operations and Information Warfare and Computational Propaganda. Partnership for Countering Influence Operations (PCIO) under Carnegie Endowment for International Peace in their research work into Influence Operations found that the terminology connected to this field is fragmented. Quantitatively, terms included Disinformation (26 percent), Influence Operations (9 percent), Propaganda (8 percent). Misinformation (6 percent) and Information Operations (2 percent).In line with this synonymous terminology, any of these terms appearing in the dissertation would be deemed to refer to SCEIIO.

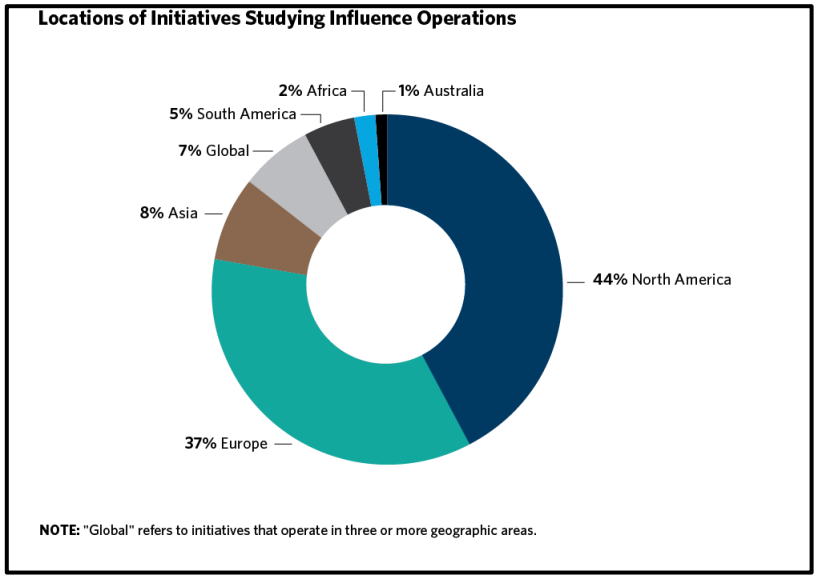


Figure 1.5 – Locations of Initiatives Studying Influence Operations

31. The vast majority of initiatives in the PCIO dataset are located in North America (44 percent) or Europe (37 percent). There are two likely reasons for this. First, North American and European countries may have more resources to fund this type of work—from large tech companies, wealthy governments, major foundations, and so on. Second, PCIO research was probably skewed toward these geographic areas due to their own limited linguistic capability and networks to reach people in Africa, Asia, and Latin America (Kamya Yadav, 2020).

32. Nearly half of all initiatives in this dataset are housed in civil society organizations (including think tanks, NGOs, charities, and other non-profits). A large role for civil society is appropriate, because influence operations prey on societal vulnerabilities that cannot be fully addressed by governments or companies alone. However, civil society's leadership in this field also represents a vulnerability. Reliance on short-term donations and grants makes it very difficult for leaders to plan

and conduct projects and recruit and retain personnel. If donors were to shift attention to other areas, a large portion of the counter–influence operations field could quickly disappear. Only a small fraction of initiatives in this dataset (5 percent) are government-run. This is striking because experts overwhelmingly believe that governments should lead the counter–influence operations effort, according to a PCIO meta-analysis of policy papers published since 2016. PCIO research could have undercounted governmental initiatives—for example, those that are not publicly announced or clearly labelled as focused on influence operations. Regardless, governments should aim to become more visible leaders in the field.

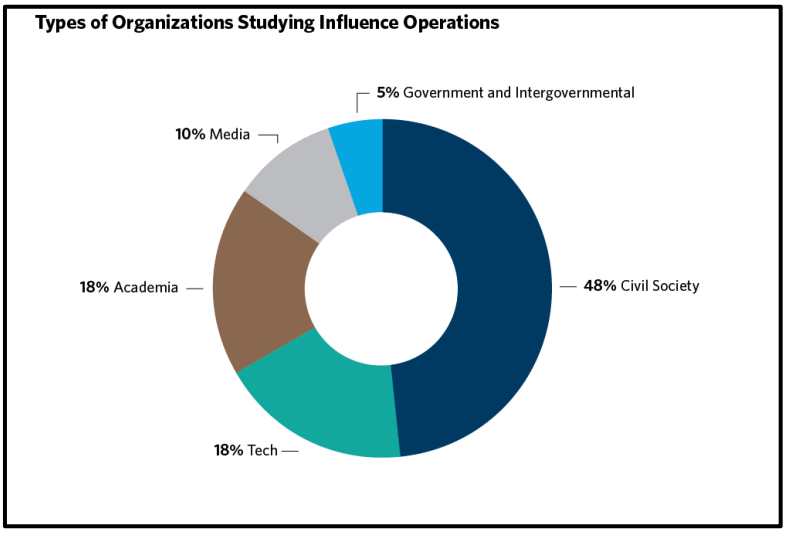


Figure 1.6 – Types of Organizations Studying Influence Operations

33. While Disinformation through cyberspace has been around for almost a decade now, suitable studies and research including its addressal by think-tanks, government bodies, NGOs, academia, etc. has not been adequate. While Cyber Security is being adequately addressed, a democracy like India has to address this issue at all levels as it has massive national security implications. Certain statistics in the preceding paragraphs point to extremely low volumes of research in this field in Asia. It also points to the fact that world over, Governments are not doing much to

support Counter- Disinformation efforts and they appear to be fronted more by civil society/NGOs presently. Hence, creation of structures at the National level for addressing Disinformation and exploiting SCEIIO as an element of National Power is extremely important. It is also important to appreciate that while the dissertation addresses organizational structures for SCEIIO, due to cyberspace being the predominant medium for prosecution of Information – Influence Ops, the structures recommended at the end would apply to the umbrella field of Information - Influence Operations as well.

Suitability of Indian National Cyber Structure to Effect SCEIIO

34. Like the US, UK and possibly other similar democracies, the paradigm of IW or IO has remained restricted to the arena of Defence Forces in India. As will be discussed later, even a marginal weaponization of the information environment can be anathema to democratic setups unlike authoritarian states which readily weaponize this environment both domestically and internationally.

35. Hence, there are Joint and individual Service doctrines for IW in Indian Defence Forces but there appears to be no extrapolation of this at the national level in a coordinated manner and at an appropriate scale keeping in view its future potential to impact or national security interests. The information environment is very much a component of what one may refer to as Comprehensive National Power (CNP) and its protection and dominance at the national and global level is a strategic imperative now. The exponential expansion of cyberspace has lent greater urgency to this as cyber enabled information influence operations can be easily conducted by adversarial state and non-state actors to harm our national security interests.

36. 2013 onwards, there was an urgency to upscale our national cyber security organizational structures. This was catalysed through issuing a National Cyber

Security Policy, 2013. However, apexed at the National Information Board (NIB) and National Cyber Security Coordinator (NCSC) at the NSCS and supported by CERT-In, National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC), STQC organizations and sectoral and state level CERTs, this structure is focused on the security of national cyberspace – the Informational and Physical Dimensions of the Information Environment but not the Cognitive Dimension. There may be capacities to conduct (S)CEITO however, conduct of SCEIIO warrants a very different organizational construct, skillset and interagency coordination. The Defence Forces with the newly raised Defence Cyber Agency (DCyA) and the Army, Navy and Air Force Cyber Groups may have conflated these two skillsets owing to legacy organizational capabilities built up as a response to prevalent IW doctrines but at the national level there is no visible conflation. While a new National Cyber Security Strategy is being formulated, it will again address the issues connected to Cyberspace Security more purposefully and expansively than its predecessor. However, conduct of Information Operations and more specifically SCEIIO may still not be addressed as it is part of a superscript which is yet to be addressed and organizationally structured at the National level.

37. With Disinformation Campaigns being writ large all over social media platforms, India can ill afford an organizational void of this nature. This study endeavours to seek possible organizational structures for Information Operations including SCEIIO at the National level, through studying other global initiatives.

CHAPTER II : LITERATURE REVIEW

" It was an extraordinary life that we were living – an extraordinary way to be at war, if you could call it war."

– George Orwell

"Hashtags are diplomacy by other means."

– Russian Sympathiser on Richard Stengel's (Head of GEC) Twitter feed

Statement of the Problem

1. India's first national level policy document connected to the information domain was published in 2013 as the National Cyber Security Policy, 2013. The first strategy level document is under formulation as the National Cyber Security Strategy (NCSS)-2021.The multifarious organizations that have been created for cyber security at the national level are largely focused on protecting Indian cyberspace and handling cybercrime. While a National Information Board (NIB) is housed in the NSC, its composition and mandate does not appear to encapsulate SCEIIO. While the Defence Forces had Defence Information Assurance & Research Agency (DIARA) (Now Defence Cyber Agency), an extrapolation of a similar umbrella organization at the national level to address the Information Warfare/ Operations domain does not seem to exist.

2. Both USA and China have restructured /created organizations in the recent past which can effectively carry out SCEIIO. Russia has already forayed deeply and effectively into this domain by not just carrying out SCEIIO during peace time but dovetailing the same with their military operations in Crimea/Ukraine/Syria. Liberal

democracies like India with socio-economic, caste, linguistic and religious fault lines are ideal fertile grounds which lend themselves to adversary SCEIIO application. The oft quoted contemporary example of classic SCEIIO is the alleged Russian interference during the US Presidential Elections in 2016 and beyond which has catalyzed creation/restructuring of organizations to counter Influence Operations. While classic Cyberspace Operations to ensure a secure and resilient cyberspace for India have been focused upon, dedicated structures and organizations are required to be created or existing organizations have to be augmented/reorganized and tasked for carrying out Information Operations in support of National Security objectives also encapsulating countering disinformation or adversary Information Operations, carried out through cyberspace i.e. SCEIIO.

4. No specific academic study has been carried out so far on the issue of creating national level structures for SCEIIO for India. Therefore, this research aims to bridge the gap by studying the same.

Research Objectives

5. The research objectives of the study are :-

(a) To understand the phenomenon of strategic cyber enabled information influence operations (SCEIIO) including Disinformation/Misinformation/Fake News/Propaganda and related technology trends.

(b) To examine the global and national trends of Disinformation and Influence Operations being carried out .

(c) To understand the organizational structures prevalent in the world (USA, EU, Russia & China) for carrying out SCEIIO.

(d) To analyse the existing cyber security related organizations in India with respect to their ability to carry out SCEIIO.

(e) To recommend policy inputs with special reference to organizational structures at the National level in India for effective SCEIIO.

Research Design

6. The study would provide insights into SCEIIO being carried out globally and responses to the same. It will enhance understanding about the varied organizational structures in countries executing and defending against such operations.

7. The study would rely on both primary and secondary sources. The primary survey would employ a semi-structured tool to interview some specialists in this field wherein some close-ended questions would be asked. However, this would be coupled with open-ended discussions and deliberations on the topic to get a nuanced opinion of the policy makers/ experts in the field. Therefore, the research approach would be primarily qualitative supported by a smatter of quantitative reasoning - the research design would be Descriptive.

Rationale / Justification

8. Till almost a decade ago Information Operations or Warfare was a largely military preserve. However, due to the ubiquity and massive expansion of social media platforms nation states have exploited these platforms to unleash Influence Operations through Disinformation and Fake News to impact the 'Hearts and Minds' of adversary nations' populace. This is not necessarily a military construct and merits a national level response and development of appropriate organizations to exploit this sub-domain of Information Operations i.e. SCEIIO at the national level.

9. The outcome of the research will provide inputs towards reorganizing/creating organizations at the National level to ensure that an important element of CNP is addressed.

Research Questions

10. The research questions that would be addressed are as under : -

(a) How the prevalent Social Media and emerging technologies including AI, Deep Fake, chat bots, IoT, etc. are having a multiplicative effect on SCEIIO?

(b) What is the difference between Disinformation/ Misinformation/ Fake news / Fake websites and the related terms that are being used for SCEIIO?

(c) What is the expanse of Disinformation and what are the global trends in execution of SCEIIO ?

(d) What are the organizational structures prevalent in the world (USA, EU, Russia & China) for carrying out SCEIIO?

(e) How effective and coordinated are the existing cyber security related organizations in India with respect to their ability to carry out SCEIIO?

(f) What are the policy changes required with specific reference to organizational structures at the National level in India for a robust ecosystem for effective SCEIIO ?

Scope / Limitations/ Delimitation

11. The research is limited to the sub-domain SCEIIO under the umbrella term Information/Influence Operations. However, the organizational structures that would be recommended would be able to encapsulate the entire spectrum of Information/Influence Operations.

Literature Review

12. Papers, articles and books for Literature Review are as follows :-

(a) **Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston - RAND (2009)** This RAND study defines influence operations in an operationally useful way, reviews the scholarly literature related to influence operations, describes the elements of a general model for effective influence operations and provides a framework for integrating influence operations into military campaigns. It also provides a description and critique of available approaches, methodologies, and tools that might assist in planning, executing, and assessing influence operations.

(b) **Sean Cordey,Centre for Security Studies, Zurich (2019)** The study seeks a definition for Cyber Influence Operations as well as a differentiation from classic Influence Operations. It also compares the American and Russian Cyber Enabled Influence Operations.

(c) **Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger - RAND(2018)**. This study focuses on Russian Influence Operations and countering it. It analysis the various tools and stages of Russian Influence Operations and models for countering it at every stage. The Russian interference in American elections in 2016 has been used as a case study.

(d) **Cyber Enabled Information Operations - Hearing Before The Subcommittee On Cybersecurity Of The Committee On Armed Services United States Senate ONE HUNDRED FIFTEENTH CONGRESS - FIRST SESSION - April 27, 2017**. The purpose of the hearing was to learn from the Russian election interference experience and other such experiences in order to assess how information operations are enhanced in terms of their reach, speed, agility, and precision, and impact through cyberspace. The hearing offers important inputs and lessons.

(e) **Martin C Libicki, Strategic Studies Quarterly, 2017**. The paper brings to fore the idea of convergence of the erstwhile Information Warfare (IW) elements and hence a focus on a converged IW threat. It argues that given today's circumstances, in contrast to those that existed when IW was first mooted, the various elements of IW should now increasingly be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations. This claim is supported by three emerging circumstances. First, the various elements can use many of the same techniques, starting with the subversion of computers, systems, and networks, to allow them to work. Second, as a partial result of the first circumstance, the strategic aspects of these elements are converging. This makes it more likely that in circumstances where one element of IW can be used, other elements can also be used. Hence, they can be used together. Third, as a partial result of the second circumstance, countries are starting to combine IW elements, with each element used as part of a broader whole. Taken together, these emerging circumstances create challenging implications for the future of information warfare. Simply put, if information

technology trends continue and, more importantly, if countries begin to exploit these trends, then as a general rule, the focus on defeating a cyberwar threat will have to evolve into a focus on defeating a broader IW threat.

(f) **Congressional Research Service – Information Warfare Issues for Congress, March 2018**. This report offers a conceptual framework for understanding IW as a strategy, discusses past and present IW-related organizations within the U.S. government, and uses several case studies as examples of IW strategy in practice. Countries discussed include Russia, China, North Korea, and Iran. The Islamic State is also discussed.

(g) **Richard Stengel, Information Wars – How We Lost the Global Battle against Disinformation & What can We Do About It, 2019**. The book is a firsthand account by Richard Stengel who was the Under Secretary of State for Public Diplomacy in the US Department of State mandated to counter ISIS and Russia in the Information Domain. It offers valuable insights into the formation of the Russian Influence Group and a Messaging Coalition against ISIS and practical problems encountered.

(h) **Herbert Lin, The Existential Threat From Cyber-Enabled Information Warfare, 2019**. The paper argues that Cyber Enabled information warfare has also become an existential threat in its own right, its increased use posing the possibility of a global information dystopia, in which the pillars of modern democratic self-government – logic, truth, and reality – are shattered, and

anti-Enlightenment values undermine civilization as we know it around the world.

(i) **Herbert Lin & Jaclyn Kerr, On Cyber Enabled Information Warfare & Information Operations, 2019**. This paper advances the idea of cyber-enabled information warfare and influence operations (IWIO) as a form of conflict or confrontation to which the United States (and liberal democracies more generally) are particularly vulnerable and are not particularly potent compared to the adversaries who specialize in this form of conflict. IWIO is the deliberate use of information against an adversary to confuse, mislead, and perhaps to influence the choices and decisions that the adversary makes. IWIO is a hostile activity, or at least an activity that is conducted between two parties whose interests are not well-aligned, but it does not constitute warfare in the sense that international law or domestic institutions construe it. Cyber-enabled IWIO exploits modern communications technologies to obtain benefits afforded by high connectivity, low latency, high degrees of anonymity, insensitivity to distance and national borders, democratized access to publishing capabilities, and inexpensive production and consumption of information content. Some approaches to counter IWIO show some promise of having some modest but valuable defensive effect. But on the whole, there are no good solutions for large-scale countering of IWIO in free and democratic societies. Development of new tactics and responses is therefore needed which the paper develops.

(j) **Ben Hatch, "The Future of Strategic Information and Cyber-Enabled Information Operations." Journal of Strategic Security 12, No. 4**

(2019). The article discusses case studies to provide an organizational framework for strategic influence. It then offers recommendations for an organizational construct to enable winning future information wars by US Govt.

(k) **U.S. Department of State, Global Engagement Centre (GEC) Special Report : Pillars of Russia's Disinformation and Propaganda Ecosystem, August 2020**. As the U.S. Government's dedicated centre for countering foreign disinformation and propaganda, the GEC at the U.S. Department of State has a mandate to expose and counter threats from malign actors that utilize these tactics. In this field, US considers Russia to be a leading threat. The Department works with interagency and global partners to meet this challenge, with the GEC playing a key role in coordinating efforts and helping lead a global response. A central part of this effort is exposing Russia's tactics so that partner and allied governments, civil society organizations, academia, the press, and the international public can conduct further analysis of their own and thereby increase collective resilience to disinformation and propaganda. This report covers this effort of GEC.

(l) **Renée DiResta, Carly Miller,Vanessa Molter, John Pomfret, Glenn Tiffert, Stanford Internet Observatory, Hoover Institution,Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives, 2020** Understanding the impact of technological innovations on China's influence operations, and how its capabilities are being deployed, is the focus of this work. This paper assesses China's media and social media landscape and seeks to answer a broader question about China's activities in terms of the

scope and nature of China's overt and covert capabilities, and how those capabilities complement one another. Evaluation of capabilities has been done through three case studies. The first case study assesses China's influence operations related to the Hong Kong protests in 2019-2020—the first time social network companies took down and publicly attributed accounts to China. The second case study analyzes China's activities during Taiwan's January 2020 election. The third case study looks at public diplomacy around the COVID-19 pandemic and China's efforts to control the narrative via both covert and overt means. Finally, a comparative framework has been applied to contrast China's activities with Russia's to better understand how these actors operate now, and to consider how China may continue to evolve.

(m) **Elsa B Kania & John K Costello, Strategic Support Force and the Future of Chinese Information Operations, 2018**. The establishment of the Strategic Support Force (SSF) in December 2015 was a critical milestone in the history of the Chinese People's Liberation Army (PLA), against the backdrop of its historic reform agenda. The SSF's creation reflects an innovation in force structure that could allow the PLA to operationalize its unique strategic and doctrinal concepts for information operations. The paper analyses the SSF through the prism of its ability to carry out effective Information Operations.

(n) **Disinformation and 'Fake News': Interim Report: Government Response to the Committee's Fifth Report of Session 2017–19, House of Commons, UK, 2019**. The report highlights the UK government response to disinformation and fake news. The Government is already undertaking work to

address a range of online harms, including disinformation. Disinformation is not a new phenomenon, but the online environment has enabled it to increase dramatically in terms of quantity, reach and speed of transmission. The response aims to reduce the impact of disinformation on UK society and UKs national interests, in line with their democratic values.

(o) **James Pamment, EU Role in Fighting Disinformation, 2020**. This paper was commissioned by the European External Action Service's (EEAS) Strategic Communications Division and prepared independently by James Pamment of the Partnership for Countering Influence Operations (PCIO) at the Carnegie Endowment for International Peace. Over one hundred experts, practitioners, and scholars participated in five days of workshops, made written submissions, and/or completed surveys that fed into this paper.

(p) **Intelligence and Security Committee of Parliament Report on Russia, UK, House of Commons, July 2020**. The report analyses the Russian Disinformation threat to the UK and countermeasures that need to be and that have been undertaken.

(q) **Credible Cyber Deterrence in Indian Armed Forces, VIF, 2019**. This VIF Task Force Report covers a large canvas of issues connected to the creation of organizational structures in the Indian Armed Forces towards achieving Credible Cyber Deterrence.

(r) **Lt Gen RS Panwar (Retd), IW Structures for the Indian Armed Forces, 2020**. In a three part series articles, the author has analyse the contemporary Information Operations/Warfare construct and recomnended structures for its effective employment.

13. **Research Gaps**. The following research gaps were found:-

(a) No major study on SCEIIO against India.

(b) National document or policy on SCEIIO or organizational structures for it in India, is not available, at least in the open domain.

14. **Method of Data Collection from Secondary Sources**

(a) Research papers and articles published by various think tanks and distinguished authors.

(b) Online open source resources.

(c) Books.

Methods to be Applied and Data Sources from Primary Sources

15. The method of research would be primarily Qualitative. An effort would be made to get Primary inputs from specialists in the field. Secondary inputs would be extracted from research papers, reports, books & articles available.

CHAPTER III : GLOBAL TRENDS IN SCEIIO

" Social Media has helped to dismantle traditional information and media hierarchies, and in so doing has given birth to a new type of hyper-empowered individual, networked, globally connected and more potent than ever before: a uniquely 21st Century phenomenon I term Homo Digitalis."

– David Patrikarakos " War in 140 Characters"

" Social networks reward not veracity but virality."

- PW Singer " LikeWar"

1. At the end of 2016, "post-truth" was named word of the year by Oxford Dictionary. It was defined as "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief." This reflected a year in which Donald Trump was on record as having told the most lies of any US Presidential candidate in modern history and in which the Brexit campaign advocating Britain's departure from the EU was largely based on a slew of misinformation and half-truths.

2. The meaning of truth itself is changing in contemporary politics and, more dangerously, in conflict, at a number of levels. First, the death of an idea of objective truth allows certain states, mostly authoritarian, through the use of propaganda, to erode trust in all sources of truth, allowing for so-called fake news to infect real news. Second, social media catalyzes both centripetal and centrifugal forces in the shaping of information: stories go viral, but you also have endless versions of events and

information overflow, both of which stretch truth like an elastic band. Third, the definition of a story is changing. Now, a tweet can itself be the story, not just a means to tell it. Finally, new rules are being created and the state lags the netizens. This explains geopolitical phenomena like the Arab Spring and the rise of ISIS (David Patrikarakos, 2017).

3. In their seminal book " Like War – The Weaponization of Social Media", PW Singer and ET Brooking outlined five core principles which form the foundation of their book, as follows:-

(a) **Internet has Left Adolescence**. The rise of social media has allowed the internet to surpass its predecessors like telephone/radio/TV as it is truly global and instantaneous – the ultimate combination of individual connection and mass transmission. It is now starting to flex its muscles and half the world has yet to come online and join the fray.

(b) **Internet has Become a Battlefield**. It is indispensable to businesses, governments, militaries, activists, spies, etc. in equal measure. They all use it to wage wars which are borderless. Every battle seems personal but every conflict is visible globally.

(c) **This Battlefield Changes how Conflicts are Fought**. Power on this battlefield is measured not by physical or kinetic means but by command of attention. The result is a contest of psychological and algorithmic manipulation, fought through an endless churn of competing viral events.

(d) **This Battle Changes What War Means**. On the internet, "war" and " politics" have begun to fuse, obeying the same rules and inhabiting the same spectrum. Their tactics and players are increasingly indistinguishable. Yet it is

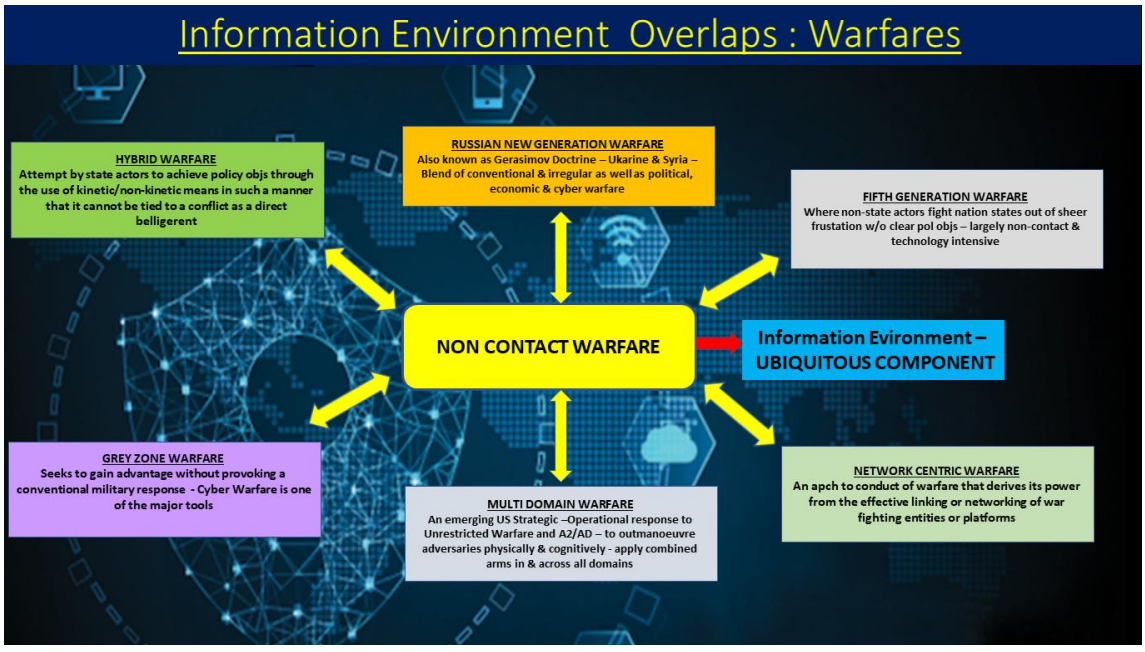
not the Generals, politicians or lawyers who are defining the laws but Silicon Valley engineers.

(e) **Everybody Online is Part of this War**. If one is online, his/her attention is contested territory. Everything that people watch, like or share represents a tiny ripple on the information battlefield. Our online attention is therefore both target and ammunition in an unending series of skirmishes.

Factors Accentuating SCEIIO

4. As great power competition has replaced the Cold War and the space for conventional conflicts appears to have diminished between near peer competitors, Non – Contact Warfare (NCW) has gained traction. The Information Environment is a ubiquitous element in conduct of various kinetic and non-kinetic forms of NCW. The non-kinetic NCW is largely fronted through the Information Environment and the advent of Social media platforms has facilitated transcending beyond classic Cyberspace Operations to Cyber Enabled Information Influence Operations. When applied by nation states or non-state actors for strategic effects SCEIIO germinated and has upscaled dramatically in the past decade.

Figure 3.1 – Information Environment Overlaps in Warfare



4. SCEIIO is characterised by certain key features which make it an extremely potent and compelling instrument across the entire spectrum of conflict. These are as follows:-

(a) **A 'Peace --- No War-No Peace --- War' Continuum**. Cyberspace provides fertile ground for conduct of SCEIIO and facilitates conduct across the Peace-NWNP-War continuum. Proxy Wars, Surrogate Wars, Hybrid Wars, etc. can exploit cyberspace effectively to achieve politico-military aims with minimum kinetic or contact operations.

(b) **Can Project Unrealistic Asymmetries**. A crippling nation state sponsored attack on critical infrastructure during crisis situations followed by a potent SCEIIO can project unrealistic asymmetries to an adversary leading to strategic paralysis.

(c) **Shapes the Public & Diplomatic Opinion & Will To Fight**. A well planned and executed SCEIIO can impact any organization or an adversary nation state and be a vehicle for the classic "Winning without Fighting".

(d) **Reinforces the David vs Goliath Syndrome**. Weaker or smaller nations with asymmetry in conventional forces can effectively employ SCEIIO for exploiting faultlines especially in democracies to sow dissension and create disruptive effects in support of conventional operations. Iran and North Korea are classic examples.

(e) **Classic Deterrence Difficult To Achieve.** The 'Pot can be kept boiling' below a certain threshold. It has been proved over the past decade that

classic deterrence is difficult to achieve in this domain as exemplified by Russian and Chinese operations against US and Europe.

(f) **Plausible Deniability – Attribution can be difficult**. Technical and political reasons especially during peacetime can make attribution and therefore a response difficult.

(g) **Cyber Domain – most potent and overarching – Non Kinetic Domain**. Today, every conventional system of news or information dissemination is encapsulated within cyberspace. In the non-kinetic domain cyberspace enjoys immense potency and is overarching. It is therefore the domain of choice for Influence Operations.

(h) **Lower cost as compared to conventional domain**. As compared to the other four domains, cyberspace operational costs and the investments would be a fraction and accrue greater dividends comparatively for the same investment.

(j) **Lack of International Norms/Laws for SCEIIO**. Conduct of SCEIIO is not covered by any laws presently as laws for operations in Cyberspace also do not exist. Certain actions on Social Media platforms do not appear to be illegal but definitely fall within the ambit of SCEIIO.

(k) **High Connectivity**. In 2020, the number of Internet users globally approached 4.6 billion people, and nearly every user on the Internet is connected to every other one through a relatively small number of links. High connectivity also means that even actors whose voice would have been small before the rise of the Internet now have megaphonic reach to large audiences. Communities of like-minded "fringe" individuals are much easier to form under such circumstances, where such individuals can and do receive social reinforcement for their views.

(l) **Low Latency**. Users that are directly linked can be notified in milliseconds of new communications and information rather than the hours or days that characterized radio, telephone, or newspaper communication.

(m) **Many-To-Many Bi-Directional Communications**. Consumers and content providers easily engage in reciprocal dialogue and the lines between consumer and provider are often indistinct. Today's information environment enables crowdsourcing—the use of large numbers of individuals acting in loose cooperation and often without central guidance to achieve certain purposes. SCEIIO originators can draw on the cooperation, witting or unwitting, of individuals whom they have been successful in influencing. In many instances, it only takes a retweet or a "like" to achieve a many-fold amplification of the message embedded in an SCEIIO operation that has influenced an individual.

(n) **Disintermediation**. Today's information environment is far less reliant on established intermediaries than the environment of a few decades ago. In the past, intermediaries such as newspapers played editorial roles that helped their readers to manage, interpret, and evaluate large volumes of information.

Today, more users depend on the newsfeeds of social media and technological tools to filter and sift information, but these tools lack serious editorial judgment. Disintermediation helps the SCEIIO originator. Those who use the online equivalents of traditional information intermediaries and rely on their editorial services to cope with the information deluge have at least some tools to cope with some SCEIIO operations because they continue to be exposed to useful and factual information from multiple points of view. But those who rely on social media and search engines to filter the information ocean are less likely to be exposed to information that contradicts their prior beliefs. These users are exposed preferentially (or almost exclusively) to information that conforms to their own individual predilections, and hence they reinforce their existing confirmation biases.

(o) **Geography Agnostic**. Because SCEIIO operations can easily cross borders, SCEIIO operators can take advantage of different laws in different geographic regions, engaging in SCEIIO operations targeted against one national jurisdiction from the comparative safety of another jurisdiction that allows such behaviour. In addition, SCEIIO originators can operate from the territories of their target nation with minimal infrastructure and gain protective benefits that the target nation confers upon its residents.

(p) **Easy Availability Of PII**. Large quantities of PII of individuals are available to interested parties, either for free or for a nominal price on the Dark/Deep Web.

(q) **Information Insecurity**. All information is subject to risks related to compromises of confidentiality, integrity, availability, and authenticity, but digitally recorded information arguably suffers these risks to a greater degree.

SCEIIO operations can exploit weak information security. Such operations can obtain information meant to be confidential or forge or alter print, audio, and video documents. The products of these operations can then be disseminated strategically to support the SCEIIO originator's objectives. An example of this approach was the Russian hacking operation conducted in 2016 to access confidential emails of the Democratic National Committee and key staffers of Hillary Clinton's campaign.

Influence Operations and SCEIIO: Similarities and Differences

3. The targets, objectives and to some extent strategies/ stratagems of SCEIIOs are similar to those of influence operations conducted throughout the last century. However, the tools, actors, scope, scale and availability, are all different.

4. **Targets**. SCEIIOs primarily target three levels of order (Pamment et al., 2018):-

(a) **General Societal Targeting**. Aimed at mass audiences by aligning messages with symbols and narratives which are widely shared by a society's population. In addition, the general society is also targeted where attacks are directed against critical societal infrastructures and institutions (e.g. the government, voting systems or energy supplies).

(b) **Socio-demographic Targeting**. Aimed at various social groups and networks, whether a region's civilian population or military personnel when used in an ongoing conflict. Messages can be adapted in keeping with general socio-demographic factors, such as age, ethnicity, profession, income, gender, or education.

(c) **Psychographic Targeting**. Entailing activities aimed at individuals selected on the basis of their psychographic profiles, be they key decision/policy-makers or ordinary citizens.

5. Influence activities can thus be differentiated between those that are increasingly "message-oriented" and tailored to specific individuals, narratives or issues, and those that are more "environmentally oriented" towards the general public and the information environment at large. Furthermore, it must be borne in mind that, while cyberattacks are directly (technically) aimed at target systems belonging to various actors (e.g. businesses, government institutions, media institutions, or political parties), such attacks invariably also have indirect cognitive effects to various degrees and at different levels. At the same time, it should be noted that SCEIIOs are not only used against foreign targets but can also be used by governments against their own populations. Indeed, during the Syrian civil war, the Assad government targeted its domestic population with social media-based propaganda in an attempt to boost Assad's standing as the legitimate ruler of Syria while trying to dissuade the population from promoting or supporting any of the rebel groups.

Objectives

6. With regard to the objectives of SCEIIOs, these remain the same as with other influence operations, namely to modify attitudes and shape the target audience's psychological processes, motivations and ideas (Palmertz, 2017). However, specific objectives are varied and depend on both context and target. They include, among others, targeting the civilian population in a particular region with dis/misinformation and cyberattacks to foment distrust toward an opponent's military and government, thus undermining the credibility of authorities and instilling a sense of insecurity.

Moreover, in a conflict situation, combatants (and civilians) can be targeted by online counter-propaganda and cyberattacks in order to reduce their willingness to fight, or even to induce them to change sides. This can also be done with a purely disruptive purpose to undermine people's psychological resilience. Conversely, CIOs can also create a positive effect by raising morale and boosting troop recruitment.

7. One of the main objectives of such operations is, however, to promote, control or disrupt a given narrative. In this regard, and according to Pamment and his co-authors (2018), the aims of influence operations can be divided into three main categories, namely constructive, disruptive, and distractive as follows:-

(a) **Constructive IOs**. Aim to (re)establish a coherent narrative (e.g. an ideology such as communism or capitalism) amongst its targets/audience. For instance, at the general level, this can take the form of mass audience ideological propaganda through various means of information dissemination. At the group level, this can entail the recruitment and promotion of adherent groups (e.g. students) to an ideology, while at the individual level it can take the shape of highly individualized, targeted political propaganda based on interest and preferences.

(b) **Disruptive IOs**. Aim to be disruptive or destructive toward an emerging or existing narrative. As such, relevant operations are often conducted via highly divisive and contested issues, such as crime and immigration. At a general level, this can mean, for instance, a general polarization of societal actors to foment distrust, while at the group level, it may involve the spreading of disinformation amongst key policy-makers in order to disrupt their decision-making and opinion-forming processes. At the

individual level, this can take the form of harassing and discouraging specific individuals from taking part in public debate or taking specific actions.

(c) **Distractive IOs**. Aim to draw attention to a specific minor issue or action in order to distract the audience from a key issue. Such activities tend to focus on the information environment, seeking to dilute, flood or poison it with alternative messages. They can, for example, be performed by hijacking public debate through false allegations or highly sensitive topics.

Cyberspace : An Equalizer And Enabler

8. The difference between traditional influence operations and SCEIIOs lies in the tools used and some of the actors involved. This is due to the new features afforded by cyberspace as an operational space. Indeed, modern SCEIIOs are able to exploit not only how information is generated, distributed and consumed on new platforms and services (e.g. social media platforms and services), but also how users and communities interact and establish relationships among themselves (Bonfanti, 2019). Specifically, the use of cyberspace has acted as a great equalizer and enabler for influence operations. On the one hand, the widespread availability and low cost of entry of cyber technologies and tools has allowed anyone and everyone to engage in influence operations, whether at a small or large scale. In terms of availability, the choice of platforms, vectors, tools, and software is huge, and most of these are easily (and cheaply) available on the internet or the Dark Web. There is, for instance, an extensive market for bots and botnets of all sorts. Meanwhile, there exists 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 different tools and new techniques (Baezner, 2018).

9. The material cost of entry to engage in such activities at the very basic level is also low. Hardware and processing power are increasingly low-cost, and one needs only an internet connection, an internet-enabled device and access to free account-based applications to start to write and spread propaganda. The only resource that can be considered costly is the time needed to set up and engage in these activities, but this can be reduced through optimization and the use of more sophisticated tools and techniques, such as automated bots and possibly artificial intelligence. In addition, the knowledge needed to engage in basic SCEIIOs is quite minimal. Indeed, only an elementary understanding and knowledge of how to use Photoshop and social media is necessary to create and spread any photomontage. This includes, for instance, widely accessible meme (e.g. Imgflip) or fake tweet generators (e.g. simitator). Accordingly, more sophisticated tools are also becoming increasingly democratized and user-friendly (Chesney & Citron, 2018). FakeApp, for example, allows extremely realistic faceswapping videos to be created using AI.

10. It must, however, be mentioned that engaging in influence operations and actually achieving their goals are two very different things. While the former only necessitates limited skills, the latter requires not only (a certain level of) precise technical knowledge and adequate infrastructure but above all a finely honed understanding of the human psyche, the context in which it operates and the function of the information and cyberspheres. This therefore constitutes a critical element for differentiating between actors with advanced capacities, preparation and intent, and bored or lonely individuals. Cyberspace also acts as a liberator from traditional controls (and intermediaries) of information, which implies that today anyone can become a propagandist. Indeed, as Cohen (2017) puts it, “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, regulation or government enforcement".

11. Traditional media and the state have lost the monopoly on information dissemination. In comparison to most social media, established news media have editorial guidelines which oversee the type and veracity of information published. Such in-house editorialization is, however, far from openly accessible. Only those with certain credentials – journalists or invited commentators – can access these outlets. Meanwhile, governments may censor or direct official/conventional media outlets in order to ensure they convey the preferred message and align with the national interests. But in contrast to these, social media and other ICT enable people to bypass these channels and circumvent censorship, as was notably seen during the Arab Spring. Conversely, this delayering and disintermediation (i.e. the loss of intervening controls, such as editors, fact checkers, reputable publishers, social filters, verifying agencies, peer reviewers, and quality controllers) has greatly helped to foster a climate prone to disinformation and propaganda in which the lines between provider and consumer are often indistinct (Lin & Kerr, 2019).

12. Overall, these transformations have allowed a plethora of new actors to engage in influence activities within the information and cyber spaces. This development has been notably reinforced by the relatively high level of anonymity granted to actors, allowing them to operate free of inhibitions (Lin & Kerr, 2019). Among them are traditional actors such as states and state-related groups as well as unconventional ones, such as hacktivists, cyberterrorists, cybercriminals and lone hackers. All of them present new threats and are driven by underlying motives which can overlap due to the multidimensionality and composition of such groups. For instance, states aim to

pursue political goals through IW and engage in a wide array of state-sponsored influence activities in order to do so. Cybercriminals, on the other hand, are primarily interested in financial profit but, as such, can also work alongside with or against governments to pursue their economic and political agendas. Cyberterrorists generally aim to exploit cyberspace to cause loss of life, major economic or political disruption, or to create a climate of fear. However, they also use this space to disseminate their propaganda; collect intelligence and funds; radicalize and recruit; and to incite acts of terrorism. Finally, lone hackers also engage in such activities for various reasons, from wanting to demonstrate their technical exploits, to seeking economic benefit or just for the thrill of challenges.

13. On the other hand, cyber-related technologies have been an enabler for influence activities in several aspects. The first being that the instantaneous nature (or low latency) of interconnected ICT and cyberspace has – in comparison to traditional state or private media, such as printed press – drastically reduced, if not nullified, the time needed to broadcast and disseminate information (Lin, & Kerr, 2019). There is no need to wait for things to be printed, delivered or parachuted. They can simply be published online on a wide variety of platforms, whether it is social media, blogs, Reddit threads or newsletters. In addition, information and messages can take a variety of forms and combinations, from text and photos to video and audio clips, all of which are easily distributed by a wide range of content providers (e.g. individuals, bots or states) and prone to manipulation and misappropriation.

14. At the same time, new cyber-related means of information dissemination have greatly expanded the possible reach and scale of influence activities at very little cost

for perpetrators, with information now able to reach a wide and geographically distributed audience and transcend traditional national barriers. Anyone or anybody having an internet connection is theoretically able to publish something capable of being read all over the world. This logic has, however, some limits, with some countries having put in place a number of measures to control and restrict this flow of international information and content for political and social control reasons, with China's "great firewall" being one of the most preeminent examples. Meanwhile, the penetration of social media varies greatly across geographical regions and segments of the population, rendering information dissemination activities highly context-dependent. As mentioned before, this ease and speed of dissemination means that the control and release of information is no longer the purview of state organizations or established private media companies. This makes control over information – e.g. for social control or political censorship – complex and resource-intensive, especially as responsibilities for relevant actions are not clearly defined. This concerns social media platforms in particular, whose responsibilities regarding the content they convey are still subject to intense discussion. While there is some legal basis for monitoring the veracity of information (e.g. in terms of services), relevant documents are mainly prepared in order to protect social media companies, ISPs and content hosts against criminal liability. The main issues are thus the speed and stringency with which they are enforced as well as the repercussions if they are not.

15. Furthermore, one could also argue that, in addition to the technical (cyber-related) component which supports the current virality of information, there is also a societal if not psychological aspect to be taken into account. Specifically, the hyperconnectivity of modern societies and the multiplicity of information platforms

and media have reinforced a natural human tendency to create, exchange and consume information and news. Indeed, being social and political animals, humans have always had a thirst for more information, news and gossip at all levels of life (e.g. friends, family, politics). In turn, new ICT, above all social media with their sharing functionalities (e.g. re-tweeting or Facebook page sharing), has enabled people to indulge in this need even further. This, alongside the commercial reconfiguration of modern media towards the attention-based business models that are infotainment and sensationalist news, has greatly boosted the propagation and speed of dissemination of information, whether true or false, across wide swathes of society. This is especially true for false information or "fake news" and disinformation, which tend to diffuse further, faster, deeper and more broadly than truths (Vosoughi et al., 2018). Indeed, this particularly concerns information relating to politics, terrorism, science and natural disasters, as it not only tends to be presented in a novel fashion (and is shared more), but is able to target, trigger and encourage emotional responses and polarized debate (Vosoughi et al., 2018).

16. This consequently makes online disinformation and propaganda campaigns increasingly effective (Paul & Matthews, 2016), and leads to a vicious circle in which information with little veracity and verifiability is widely shared and then accepted both within and outside social groups, exploiting what some experts call the "illusory truth effect", in which repetition leads to familiarity and thus acceptance. Specifically, the information overload that is concomitant with online information and the internet causes a certain cognitive laziness among users, meaning that they employ various different heuristics and shortcuts to determine whether new information is trustworthy (Paul & Matthews, 2016). Moreover, the development of computer technologies and

bots has helped create a sense of legitimacy, allowing fake news to appear legitimate and real, as fake stories are pushed, circulated and engaged with and thus accrue a false sense of social capital (Pamment et al., 2018).

17. SCEIIOs of this type are also increasingly effective and optimized as the use of targeted online advertisements has allowed for an increasing penetration, precision, and personalization of information targeting. As mentioned earlier, ongoing technological advances, notably in AI technologies, the architecture of the internet and the widespread use of social media platforms (and other apps) have greatly facilitated the collection, analysis (again by AI) and exploitation of psychographic data by states as well as private companies. These technical affordances have enabled the creation and distribution of information (ads or messages) using highly personalized models of contemporary information influence activities at an unprecedented level. One striking example is none other than the Cambridge Analytica scandal, in which personal data of 87 million Facebook users was improperly shared with the company. The data 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 India, Kenya, Malta, Mexico, the United Kingdom (i.e. the Brexit vote) and the United States (i.e. the 2014 midterms and 2016 presidential election). These targeted activities relied on a number of existing algorithmic recommendations tools (e.g. on Facebook and YouTube) to feed information confirming or reinforcing existing cognitive biases thus creating an increasingly fragmented information sphere which could then be exploited by actors benefiting from the promotion of wedge issues.

18. On a more general side note, it seems important to recognize the dual use and implications of the above-mentioned technological and societal developments. Indeed, whilst most of these have acted as great equalizers and enablers of influence operations, thus reinforcing the offensive-oriented side of cyberspace, they can also be used for counter-influence efforts. This is increasingly the case with AI, which is now used for the (early) detection of influence campaigns and in-depth analysis of (social) networks. With regard to SCEIIO, Pamment et al. (2018) have devised the following list of techniques and tools most commonly used. Most of these tools and techniques are derived from traditional ones, but have been enhanced through cyberspace: -

(a) **Sociocognitive (Communities) And Psychographic (Individual) Hacking**. Aims to get inside the mindset of a person or group by exploiting cognitive vulnerabilities, psychosocial trigger points and emotions (e.g. fear, anger, hate, anxiety, honour, etc.) to influence their behaviour. Contrary to marketing campaigns, cognitive hacking is conducted with the intent to covertly influence an audience and does not need to offer any coherent narrative or even be based on fact in the middle to long term. This is powerfully illustrated by the practice of "swiftboating", in which politicians are subjected to timely smear attacks just before elections without giving them a possibility to respond. One example of sociocognitive hacking was the 2013 social unrest and violence that ensued in India after social media, specifically WhatsApp, helped spread rumors (through an unrepresentative video) which led to severe interfaith violence (Magnier, 2013). Psychographic hacks, in contrast, target individuals by isolating them and mostly rely on the collection of big data and the provision of commercial services by social media platforms such as Facebook (Pamment et al., 2018). Specifically, psychographic data can

be used to design interventions based on individual sentiments. One example are *dark ads,* i.e. ads only visible to the user and designed to influence (e.g. politically) on the basis of their psychographic data. However, the identities of those targeted, and the messages they are targeted with, remain clandestine, rendering such influence operations highly potent and discreet. Psychographic ads were, for instance, used on Facebook and paid for by the Internet Research Agency (IRA), an organization with alleged links to the Kremlin, during the 2016 US presidential election. Most of its (over 3000 types of) ads focused on controversial topics (e.g. race, gay rights, gun control and immigration) to further polarize the political debate and public (DiResta et al., 2018).

(b) **Social Hacking**. Aims to exploit vulnerabilities arising from sociocognitive features of the human mind, notably our tribal nature and drive for in-group conformity. This is particularly prevalent on social media, where humans are vulnerable to the exploitation of various group dynamics. Social hacking can be categorized into three main groups: harnessing social proof, the bandwagon effect, and selective exposure. The first involves the exploitation of people's tendency to believe something not based on sound arguments but because a lot of others seem to believe it (Pamment et al., 2018). In this regard, likes and recommendation algorithms in social media are primed to push disinformation and propaganda more readily than other types of information. The second effect relates to the known phenomenon of ideas self-amplifying and becoming more widely accepted to an ever greater degree the more "popular" they become. While present in many domains (e.g. fashion), this phenomenon is especially preeminent in politics, where 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" (Pamment et al., 2018), is widely used. Lastly, 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 referring to a state of intellectual isolation resulting from algorithmic personalization and the latter describing "organically created internet sub-groups, often along ideological lines, where people only engage with others with which they are already in agreement" (Bright, 2016). These can lead to polarization, a fragmentation of online opinion and political division, particularly given that social media are increasingly used as media sources and platforms for information, as well as for the reinforcement (radicalization) of existing ideologies.

(c) **Para-social Hacking**. This refers to the exploitation of para-social (i.e. illusionary) relationships, which occur when individuals experience one-sided relationships as being two-sided (i.e. symmetrical and reciprocal). Social media, such as Instagram, Twitter or Snapchat, and the celebrity culture have allowed everybody to build immediate and intimate para-social relationships with strangers, celebrities and decision-makers, enabling them to share information and messages directly, bypassing the scrutiny of classic gatekeepers such as journalists. In this context, there are three possible forms of exploits: influencers providing information directly to their followers (fake friends); friendship networks (e.g. Facebook) being exploited to share content uncritically, thus contributing to the spread of propaganda or disinformation (faked friendly); and propagandists posing as ordinary people, making their

messages less threatening, seemingly more authentic and more easily shareable.

(d) **Disinformation**. This is an ancient technique based on the distribution of false or partial information intended to mislead and deceive. The term remains highly contested and elusive in both relevant literature and the public debate, and the popularization of new terms such as "fake news" has not helped the discussion. For the purposes of this analysis, disinformation strictly refers to "news articles that are intentionally and verifiably false and could mislead readers" (Allcott & Gentzkow, 2017). As mentioned earlier, digitalization has had a powerful impact on the ease, speed and effectiveness with which disinformation is created and disseminated. Without going into excessive detail, one can differentiate several types of disinformation, ranging from slightly illegitimate activity regarding selective facts to the disruptive creation of fake news outlets. More specifically, disinformation activities include *advertising, satire, propaganda, misappropriation, manipulation* and *fabrication* (Pamment et al., 2018), with the degree of illegitimacy escalating as follows: selective facts < out-of-context information < lying < creation of false facts < denial of attempts to correct < creation of fake platforms or media.

(e) **Forging & Leaking**. This refers to the illegitimate dissemination of falsified evidence (e.g. on social media or the Dark Web) with the aim of propagating falsehoods, fuelling misleading narratives, and discrediting associated parties, as well as "cultivating distrust among citizens and inducing them to question the integrity, reliability and trustworthiness of the media" and

public institutions and figures (Pamment et al., 2018). Relevant activities can include the use of fake letterheads, official stamps and signatures, sometimes combined with the leaking of secret communiqués (Pamment et al., 2018).

(f) **Potemkin Villages of Evidence**. This refers to the attempt to set up intricate institutional networks that are controlled and used by actors as a fact-producing apparatus for the promotion and amplification of specific narratives. Potemkin villages can, for instance, consist of an array of illegitimate or fake research, (online) journals, NGOs or think tanks that produce studies, working papers, conferences, etc. to present the respective narrative as a product of careful scholarly consideration. As such, they tend to exploit the *Woozle effect,* which refers to seeing what one is expected to see rather than what is actually there, and assuming that well-referenced sources are necessarily true (Pamment et al., 2018). Persistent examples in Western literature are the Russian-sponsored online journals RTnews and Sputnik. However, it should be noted that these are not the only ones, and some Western online news could also be considered to fall within this category.

(g) **Deceptive Identities**. This refers to the exploitation and transfer of legitimacy from a legitimate actor or platform to an illegitimate one by *shilling, impersonating* or *hijacking* (Pamment et al., 2018). Shilling involves a person engaging with a particular subject (e.g. through marketing or a review) jointly with the actor concerned, for example someone writing a glowing customer review or answering their own questions under different identities to simulate a debate. Impersonators, as suggested by the term, pretend to be someone else (whether online or offline) to better spread

disinformation, while hijacking refers to websites, hashtags, memes, events or social movements being taken over by a hostile or other party for a different purpose, whether to disrupt or to disseminate disinformation. Deceptive identities can be generally grouped into first-hand (i.e. actors assuming the role of someone else) or second-hand identities (i.e. actors assigned an identity by someone else, e.g. being cited as an expert in matters outside their sphere of knowledge) (Pamment et al., 2018).

(h) **Bots & Botnets**. Short for robots, bots refer to "a piece of automated computer software that performs highly repetitive tasks along a set of algorithms" (Pamment et al. 2018). There are myriads of bots, many of which can be and are used for legitimate and useful purposes (e.g. crawler, monitoring, aggregator, or chat software), but a number of bots are used for nefarious reasons, such as spreading disinformation and illegitimate content, price scraping, spamming forums, web analytics, DDoS, distributing malware, and other scams (Pamment et al., 2018). As such, bots are powerful tools used to support information influence activities, as they can easily mimic organic behaviour in order to mislead, confuse and influence publics beyond their own social networks. In terms of influence operations, there are four main social bots in use: hackers, spammers, impersonators and sockpuppets. 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 (Pamment et al., 2018), while sockpuppets are semi-automated lookalike or imposter accounts controlled and coordinated by individuals to conduct false-flag operations or to disseminate disinformation. Overall, social bots and botnets can act as very efficient amplifiers for other influence techniques at a very low cost. They are able to exploit social and cognitive (cf. band wagoning) as well as technical vulnerabilities of social media platforms (e.g. trending algorithms, friend lists, recommendations or hashtags) to reinforce the virality and penetration of specific messages and narratives.

(i) **Trolling & Flaming**. Refers to users of (or social bots on) online social platforms deliberately trying to aggravate, annoy, disrupt, attack, offend, or cause trouble by posting provocative and unconstructive content (Moreau, 2017). Trolling generally targets particularly naïve or vulnerable users, while flaming aims to incite readers in general (Herring, 2002). A distinction is generally made between classic and hybrid trolls, with the former being ordinary people engaged in trolling for the sake of some personal motivation or attention-seeking. While often not fundamentally politically engaged they can, however, be recruited by actors within the context of information influence campaigns to unwittingly contribute to the spread of disinformation. The latter operate under the direction of someone else, most often an organization, state or state institution (NATO, 2016) with a clear instrumental purpose often connected to communicating a particular ideology to a particular target audience in a systematic manner. They include both the highly organized trolls working in “troll factories” and individual trolls operating in a less organized

manner under the influence of someone else. As such, trolling and flaming are particularly potent in polarizing debates, silencing opinion, distracting online debate and generally disrupting the formation of public opinion (Pamment et al., 2018).

(j) **Humour & Memes.** Refer to the use of humour as a "communication tool that entertains, attracts attention [and] serves as light relief" (NATO, 2017), but which, at the same time, also serves to covertly manipulate and influence "hearts and minds" to advance goals and agendas not recognized by the audience. Indeed, humour is particularly powerful, as it causes people to be less guarded and more open to sensitive issues. It can influence ideas, which then shape beliefs, and subsequently generate and influence political positions and opinions. On the internet, a commonly used and potent vector for humour and influence are "memes", which are more than just funny pictures with jokes written on them. Indeed, they are expressions of shared cultural ideas, making them immediately appealing and thus hard to avoid. Furthermore, their interpersonal, ambiguous and ready-to-be shared simplistic design gives them not only a high viral potential but also a high acceptance potential (as they come from within people's own social networks, cf. availability bias). As such, they are ideal tools for legitimizing fringe or controversial ideas, opinions and narratives, and for ridiculing, humouring and joking to "weaken monopolies of narratives and empower challenges to centralized authority" (Pamment et al., 2018). Other related examples include humouristic GIFs, caricatures, and videos.

19. Overall, SCEIIOs and relevant campaigns use a variety of strategies, most of which were deployed by traditional influence operations in the past but now find themselves enhanced by cybertools. The following is a non-exhaustive but synthetic list of such strategies (Pamment et al., 2018):-

(a) **Black Propaganda**. The creation and dissemination of fake evidence through social media to spark social outrage.

(b) **Point and Shriek**. Takes advantage of the extreme sensitivity of certain groups in contemporary society, in particular groups that are often also highly active on social media and well aware of the viral dynamics of the hybrid media space.

(c) **Flooding**. This is a strategy in which the information space is overloaded with conflicting information to hamper the assessment of information credibility.

(d) **Cheerleading**. Operates in the same manner as flooding but with a limited number of more or less spuriously substantiated *narratives,* pushed via multiple channels and amplified by *botnets,* in order to overload the target system's capacity to differentiate credible from non-credible information.

(e) **Raiding**. This is a coordinated attack on an information arena to crowd out and silence opinions and exhaust others through disruption. This can be achieved via a variety of tools, such as spammer bots, trolls or DDoS attacks.

(f) **Polarization**. Has been observed during the US election. This strategy aims at supporting two extremes of a specific issue to force mainstream opinions into one of the two. To achieve this, a wide array of tools can be used, from social and parasocial hacking to trolling, disinformation and memes.

Potential & Strategic Implications : SCEIIO

20. As shown by the increasing use and research, cyber influence activities, whether cyber-enabled influence activities or cyberattacks in support of influence activities, have gained considerable traction in recent years, as both large and small actors have come to recognize their potential. This trend will surely continue in the future. More specifically, SCEIIOs are particularly attractive as they represent a good counterbalance to conventional power (at little cost yet large flexibility) with low risks of detection and escalation but high potential results. Indeed, as mentioned previously, the cost of entry and resources of SCEIIOs, whether in terms of hardware, software or knowledge, is very low in comparison to traditional influence operations. Cyber Influence tools are easily available and affordable. In addition, a wide variety of them exist, many of which are inter-operable, allowing for great operational flexibility and fluidity. An actor is thus not only able to easily vary and adapt the frequency, scalability and intensity of their operations, but also to precisely tailor them to the required context and targets (Cronin & Crawford, 1999).

21. Cyber influence capabilities in particular present a number of interesting features for nation states' influence operations. Indeed, they are inherently versatile, ubiquitous and uniquely secretive, allowing states to operate in the grey area between

peace and war. They are also incredibly flexible in their use and can in certain cases even substitute conventional and unconventional capabilities. As such, they can be used for standalone or support operations. Potential applications include, among others, preparation for kinetic battle (e.g. during the 2008 Russo-Georgian war) or "intelligence, reconnaissance, surveillance and psychological operations, as well as for signalling deterrence, for discreet sabotage and for widespread disruption" (Blank, 2017). Besides, the same tools and exploits can be used for multiple purposes and be further improved over time (e.g. the BlackEnergy series of Trojan software). In addition, cyber tools present other advantages in that they can be turned on and off according to need (and context) and are mostly non-lethal (cf. international law implications), temporary and reversible, which further reduces the risk of escalation.

22. In turn, these factors and the rapid growth of communication technologies underpinned by social media have provided a great number of (new) actors (small non-state as well as state) with a way to (counter)balance conventional capabilities of conventionally powerful states and further their political and strategic interests without the use of force. This is especially true for small non-state actors which, given their size and internal processes, have relatively high operational agility compared to established bureaucracies when it comes to accessing and utilizing new technologies.

23. At the same time, SCEIIOs present a limited risk of escalation for state actors because they do not constitute a "use of force" under existing international law, which would trigger retaliation and self-defence. The only exception would be, according to the non-binding Tallinn Manual, high-end cyberattacks causing physical harm and destruction. As such, most SCEIIO activities are conducted in the grey area between war and peace, and they are usually not prohibited under international law, which

considers them as hybrid threats alongside other types of non-military threats such as disinformation and diplomatic, economic or military pressure. Similarly, many of the cyber-enabled influence activities used to exert political influence in democratic countries are legal (e.g. big data, dark ads, social bots).This is particularly true as under customary international law a state can only be trialed for breaching its international obligations, for instance violating another state's sovereignty or the principle of non-intervention, if its responsibility as an actor can be confirmed. In other words, it is necessary to determine whether that state exercises "effective control" over the group or organization conducting the influence operations in question (Pernik, 2018). Cyberspace, however, makes it complex to do so. The problem is thus threefold, namely one of detection, scrutiny and attribution.

24. Indeed, detecting middle to high-end cyberattacks in support of influence operations can be difficult. Attackers can often operate undetected over long periods of time, with the average time to detection of cyberattacks being 200 days (Pernik, 2018). Low-end cyberattacks, such as DDoS or social media hacks, are, however, by their nature much more visible. With regard to SCEIIOs, such as social media and dark ads, their detection can be somewhat difficult, at least for the targeted audience. This is even more true as actors engaging in influence operations on social media can count on the – more or less subconscious – support of "useful idiots", i.e. users, who uncritically process and disseminate information further, thus amplifying the magnitude of the respective operation while blurring the traceability of such SCEIIOs (Bonfanti, 2019; Lin & Kerr, 2019). One must however note that the new social media transparency guidelines enacted and enforced after the 2016 US elections have somewhat improved traceability, at least with regard to money trails.

25. On a strategic level, it is, however, problematic to determine the efficiency and direct/indirect cognitive effects these cyber influence operations have on populations and politics with any degree of certainty. As a result, analyzing their effects and their perpetrators' possible intentions (or plans), and understanding their intended messages is highly subjective and difficult to prove based on sound evidence, mostly because of secrecy (Pernik, 2018). Indeed, as Allcott & Gentzkow's study (2017) has shown, it is possible, though potentially difficult, to measure changes in opinion or behaviour or shifts in government policy resulting from SCEIIO from a methodological perspective. Nonetheless, given the ambiguities surrounding cyberattacks, a negligible cause-and-effect relationship between specific cyberattacks and shifts in public opinion can certainly be assumed (Pernik, 2018).This lack of observable and tangible effects limits the available response options in turn. To date, there have only been out-of-domain overt responses to foreign SCEIIOs in times of peace, and their effectiveness still needs to be proven. Such responses include, for instance, the diplomatic and economic sanctions enacted against Russia by the Obama administration after Russian interference in the 2016 elections. Moreover, when it comes to Western countries, the legality of and capabilities (e.g. resources, language and cultural knowledge) for possible in-domain responses remain highly debatable. In times of war or conflict, in contrast, greater escalation and stronger responses have been observed, with the US online counterpropaganda efforts against ISIS constituting a notable example.

26. For its part, information scrutiny and monitoring is made increasingly difficult by the widespread use of social media and their inherent designs, which tend to

promote the dissemination of information without any regard for the review or traceability of sources. Memes, photos and videos are particularly good vectors, as they offer only fragmented information without ascertainable factual content or identifiable source but are widely shared by friends or promoted by social media algorithms. Furthermore, the fast-moving nature of social media and information technologies requires states (or interested parties) to assemble a wide array of (evolving) techniques and technologies to quickly identify, monitor, and counter adversaries' influence operations.

27. Meanwhile, the attribution of specific cyberattacks or influence operations often remains difficult, given the prevailing anonymous targeting in cyberspace, thus allowing for a certain degree of plausible deniability even where the source of an attack has been more or less established (Brangetto & Veenendaal, 2016). This is notably the case with online propagandists, who are able to hide behind pseudonyms and automated botnets, as well their freedom of opinion, when pilloried. There are, however, a number of caveats to be taken into account when considering the potential of SCEIIOs :-

(a) First, that CEITOs in support of CEIIO can easily spiral out of their operators' control. The use of sophisticated malware can, for example, be a wild card, as once such malware is in the open, it is uncertain whether it will achieve the desired effect, and there is always the possibility that an operation may backfire. Adversaries may replicate, reverse-engineer or proliferate malware, for example, in order to use it against the original owner.

(b) Second, the striking power of CEIIOs cannot be compared to that of nuclear weapons, for example. Indeed, the power these operations wield is primarily psychological in nature, and part of the target population may therefore be immune to their effects. This is particularly the case where the rule of law is underpinned by strong institutions and traditions (Lin & Kerr, 2019).

(c) Third, the effects of cyber operations are difficult to foresee and limit to specific targets, with the exception of highly sophisticated cases (e.g. Stuxnet). The level of downstream escalation (e.g. political or diplomatic) is always uncertain. Once an attack is launched, it can result in unintended consequences, go viral, cause unexpected damage or even have the opposite effect in the long term, for example by raising awareness of the issue concerned.

(d) Finally, the real medium to long-term strategic impact of CEIIOs is difficult to assess. Indeed, as mentioned earlier, their intent, effect and objectives are not only difficult to observe but also to measure. Furthermore, the chaotic/inconsistent and operational forces that seem to drive these operations raise the questions of the necessity for strategic thinking in this regard, and, most importantly, the associated costs.

SCEIIO Trends of Major Players

28. From a methodological standpoint, the USA and Russia have been chosen (Sean Cordey, 2019) because relevant literature identifies them as the two states with the most highly developed and mature information warfare and influence operation strategies and tactics. While the People's Republic of China and the United Kingdom have also developed similar capabilities, they are not examined here due mainly to a lack of open sources and the limited scope of this study. Meanwhile, there is an extensive body of literature (mainly from Western sources) on Russian and American information and influence warfare, which has focused increasingly on cyber influence operations since the 2016 US presidential election and the various elections in Europe the following year. As a result, there are a number of open-source documents in the form of testimonies and reports by various institutions, on which this analysis and comparison is based. This method, however, entails a number of caveats, notably concerning the veracity and accuracy of these sources, which can never be fully guaranteed. Moreover, a certain bias regarding Russian operations must be kept in mind, as most of the literature comes from the West, whereas Western influence operations are only openly described and studied in a limited fashion and only in what is considered a legitimate context, namely war. A final but important caveat is that the comparison is based on political attribution, which is not always confirmed (including technically).

29. With that in mind, the analysis referred (Sean Cordey, 2019), thus compares six cases of Russian SCEIIOs and four by the USA (including its involvement in NATO operations), all of which are situated at different points on the scale ranging

from peace to war. At the highest end of the scale, there are six wars, namely the 2008 Georgian war; the Ukrainian conflict since 2014; the NATO and US operations during the wars in Kosovo (1998), Afghanistan (2001–present), and Iraq (2003 – 2011); and the military intervention against the Islamic State of Iraq and Syria (ISIS) (around 2015). The analysis additionally includes two cases of geopolitical tensions in the 2007 Estonian cyber operations and the 2015/2016 Russo-Turkish crisis following the Sukhoi Su- 24 shoot down and the assassination of the Russian ambassador. Lastly, it also includes two cases of election meddling, namely in the US and French presidential elections of 2016 and 2017 respectively.

SCEIIO During Conflicts

30. Open conflicts are prone to the deployment of SCEIIOs. Among the conflicts examined, the Ukrainian conflict and the military intervention against ISIS stand out as those in which the broadest range of operations were conducted, including tools and techniques pertaining to both types of CIOs. However, these did not take place in isolation from the remaining approach taken by security forces in either of these conflicts, which entailed a military and tactical operative dynamic on the ground as well as in cyberspace.

31. The Ukrainian conflict involved the most extensive hybrid warfare operations with a combination of a wide array of tools, ranging from massive propaganda efforts (notably on social media) to highly sophisticated hacks (i.e. the 2015 attack against the Ukrainian power grid) and the use of troll farms. Most of Russia's cyber operations (e.g. Operation Armageddon) were highly coordinated and systematic and

largely coincided with Russian military strategic interests in the region. The various CIOs in this conflict targeted a highly diverse group of actors, from enemy military personnel and the general population to media outlets and state institutions alongside international institutions such as NATO. Accordingly, they served a great variety of objectives, both nationally and internationally, depending on the targets. This notably included demoralizing enemy troops; encouraging allied forces; instilling distrust and skepticism toward the Ukrainian government; controlling a given narrative; and discrediting political and military figures. In addition, this conflict is the only known case in which a highly sophisticated cyberattack was conducted (against the Ukrainian electricity grid). Furthermore, it is also the only case in which doxing was reported (e.g. Catherine Ashton's telephone recording or the American ambassador's correspondence, to cite just a few), as well as one where narratives were manipulated to deny specific actions, such as the presence of Russian troops in Donbass or the downing of flight MH17 in 2014.

32. The military intervention against ISIS, in contrast, was a game changer for the USA as far as CIOs are concerned. There is wide agreement that ISIS's omnipresence on and capacity to act via social media (e.g. for propaganda, recruiting, raising funds, etc.) was a wake-up call for the USA to reclaim the information space. As a result, the USA developed various responses, including CIOs notably SCEIIOs focusing on social media messaging, such as the "think again, turn away" campaign. The USA further runs activities in various agencies across the state, including the US Department of Defense's (DoD) WebOps (part of CENTCOM), which focus on disrupting and countering ISIS propaganda; exposing ISIS hypocrisy and crimes, notably through the use of defectors to prevent recruitment; and mobilizing ISIS opponents (Parrish, 2016). Alongside these, the Department of State disseminates its

messages and narratives through its network of unidentified actors and individuals (e.g. foreign governments or leaders of Muslim communities) to reach a wider audience (Tucker, 2016). In contrast to the Ukrainian conflict, CEITOs such as DDoS, defacement and doxing were used relatively less frequently, or at least have not been openly reported. There were cases of hacks, including the 2016 Operation Glowing Symphony, which served a range of purposes from destroying propaganda material to instilling a sense of insecurity, and deceiving and forcing individuals to expose their positions (before being targeted by drones) (Cohen & Bar'el, 2017). The long-term effectiveness of these operations has, however, been widely debated. As in the Ukrainian conflict, CIOs targeted a broad range of actors at multiple levels, from ISIS combatants and propagandists to groups at risk of falling for ISIS propaganda.

33. On a more general note, SCEIIOs conducted by Russia and the USA differ in terms of the actors performing them. Indeed, Russia seems to (or at least used to) collaborate with external actors for low-end cyberattacks. This was notably the case first in Estonia in 2007, and then in Georgia a year later. In both cases, links could be established to the criminal/mafioso organization the Russian Business Network (aka. R.B.N.) (Blank, 2017). In the Georgian conflict, relevant activities were closely coordinated with Russian military operations, with times, tools and targets being listed on hacker forums. SCEITOs served as first strikes to degrade the Georgian government's ability to counter the Russian invasion by disrupting communications between it and the Georgian people, stopping a large number of financial transactions, and causing widespread confusion (Blank, 2017). The involvement of Russian patriotic hackers called the Nashi Youth Movement has also been reported (Baezner & Robin, 2018). While this group was officially disbanded in 2012, it is suspected that former

members have continued to perpetrate cyber-activities against what they perceive to be enemies of Moscow, notably in Ukraine (Denning, 2011).

34. Georgia was therefore Russia's first attempt to combine kinetic and cyberattacks against command-and-control and weapons systems on the one hand, and information psychological attacks against media, communications, and perceptions on the other (Blank, 2017). In Ukraine, it is suspected that the Internet Research Agency (IRA), an organization with alleged links to the Kremlin, took up the RBN's activities alongside social media-related SCEIIOs (e.g. trolling, bots, misinformation, etc.). Sophisticated hacks have, however, been attributed to pro-Russian hacker groups (CyberBerkut), who have not been proven to have direct links to the Russian state but are suspected to be the Russian cyber espionage group APT28 (Bartholomew & Guerrero-Saade, 2016). The implication of military units is not disclosed, but highly likely.

35. In contrast, the US tends to rely mostly on its diplomatic, military and domestic personnel to perform SCEIIOs. As mentioned earlier, these include the DoD's US CYBERCOM and CENTCOM, the DHS's Countering Violent Extremism task force and the DoD's Center for Strategic Counterterrorism Communications (from 2011 to 2016). The US has also been known to outsource some of its activities to contractors. This is for example the case with Operation Earnest Voice, an astroturfing campaign operated by CENTCOM but developed by the web security company Ntrepid. The campaign is aimed at using sockpuppets to spread pro-American propaganda on social

networking sites based outside of the US, notably in Pakistan, Afghanistan and Iraq (Fielding & Cobain, 2011).

Table 2: Comparison of US and Russian CIOs (author's design)

Legend: x reported o probable/uncertain	Kosovo (1999)	Iraq (2001 – 2011)	Afghanistan (since 2003)	Estonia (2007)	Georgia (2008)	Ukraine (since 2013)	Turkey (2015/16)	ISIS (since 2015)	US elections (2016)	FR elections (2017)
Point of view	*USA*	*USA*	*USA*	*RUS*	*RUS*	*RUS*	*RUS**	*USA*	*RUS*	*RUS**
CeTIO										
Technical sophistication	med.	med.	med.	med.	med.	high	low	med.	med.	med.
DDos/DoS				x	x	x		o	o	
Defacement			o	x	x	x		o	o	
Doxing						x			x	x
Hacks	o	x	x	x	o	x		x	x	x
Highly sophisticated hacks						x				
CeSIO										
Cognitive hacking						x	o		x	o
Social hacking		x	x			x	x	x	x	x
Parasocial hacking		o	o			x		x	x	x
Disinformation	o	x	x		x	x	x	x	x	x
Forging & leaking						x			x	o
Potemkin		x	o			x	x		x	x
Deceptive ID		x	x			x	x	x	x	o
Bots/botnets/sockpuppets		x	x	x	x	x	x	x	x	x
Trolling & flaming					x	x	x	x	x	x
Humor & memes						x			x	x
Targeting										
Population		x	x	x	x	x	x	x	x	x
Military personnel	o	x	x		o	x		x		
Policy-makers/personalities		x	o	x	x	x	x	x	x	x
Other communities/groups					x	x		x	x	x
Individuals		x	x			x	o	x	x	o
Objectives										
Disrupt activities – sense of insecurity	o	x	x	x	x	x	x	x	x	x
Control/reinforce/redirect narrative		x	x		x	x	x	x	x	x
Undermine trust in institutions/ media/ allies		x		x	x	x	x	o	x	x
Demoralize/encourage			x			x		x		
Sow division/polarize						x	x		x	x
Nudge policy				x		x			x	
Discredit/support individuals		x				x	x		x	x

Fig 3.2 – Comparison of USA & Russia CIO (CeTIO are SCEITO & CeSIO are SCEIIO)

36. A comparison of targets and objectives of SCEIIOs shows that military personnel are most commonly targeted during conflicts, whether by cyber-enabled tools or cyberattacks, with operations serving a range of purposes, including demoralization, the creation of uncertainty, deception, and motivation. One example is the dissemination on social media of videos shaming captured Ukrainian soldiers.

Furthermore, in all of the studied cases, the population at large is also commonly targeted by propaganda and various disinformation campaigns, whether in order to push, repress or counter various narratives. Specific individuals (e.g. politicians, leaders, propagandists, etc.) of strategic interest are frequently targeted by cyber-attacks for disruption, intelligence or pressure purposes, as are various institutions (e.g. financial, government, media), which are prime targets for DDoS attacks that cause operational and communicational paralysis and undermine the population's trust in these institutions, as was the case in Georgia. Lastly, lone hackers and groups have also been targeted (i.e. in hacker wars). While the aims of such attacks tend to be tactical and strategic in nature, they still have some cognitive effects (e.g. disruption or demoralization), as has been observed in Georgia, Ukraine, and against ISIS.

37. In terms of tools and techniques, the comparison shows that disinformation and propaganda are widely used by all actors to disrupt and control their narratives. While some channels vary, the US and Russia mostly use the same ones but at a different scale. These include, among others, online news outlets (i.e. Potemkin news), social media and sockpuppets amplified by bots. While Russia's use of propagandist online news platforms (e.g. Sputnik or RTnews) is well documented, it has also been reported that the US Departments of Defense and State have published, supported and in some cases (i.e. in Afghanistan) co-opted a number of media to support their narratives. Online, both states use social media and bots to amplify their messages, but while the US officially/publicly only operates several hundred state-related accounts on various platforms, it can be reasonably expected that Russia, through its troll farms and the IRA, operates more. The extent to which sockpuppets are used by both sides remains unclear, but it has been shown that both use them

relatively extensively (e.g. as part of Operation Earnest Voice and in Ukraine). Meanwhile, memes and humour appear to be SCEIIO tools used by Russia alone for propaganda purposes, as the US does not seem to have seized memetic warfare as yet.

38. A final observation to be made is that the US seems to have been relatively slow to adopt internet-based influence operations or PSYOPS compared to Russia's use of SCEIIOs, at least in the first decade of this century. Indeed, Russia understood quite quickly after the second Chechen war and the Georgian war that control over information in cyberspace was critical for the effective execution of its military operations . This led to an experimentation with various tools and techniques, notably during the Snow Revolution in 2011, which were then later used in Ukraine. Meanwhile, according to a RAND report (Munoz, 2012), internet-based PSYOPS were not really considered in Afghanistan or were at least deemed too ineffective against the Taliban. This must, however, be seen in the context of the Iraq and Afghanistan wars, in which the use of cybertools was evidently unsuitable, given both countries' low internet penetration of only around 5% each in 2011 (World Bank & International Telecommunication Union, 2019). However, a transition of certain PSYOPS to the online sphere could still be observed, for example via the *radio in a box* (RIAB) program or newspapers going online. While this transition might have not materialized in these cases, DoD strategists have been talking of seizing the opportunities afforded by the internet and information technologies to improve the range and efficiency of PSYOPS and propaganda since at least 2003, when they published the Information Operations Roadmap –Rumsfeld's Roadmap to Propaganda (US DoD, 2003). That document specifically aimed to provide the **DoD with a plan for advancing information operations as a core military competency by**

expanding and coordinating both military PSYOPs and public diplomacy operations (US DoD, 2003). It underlined the need for rapid, wide-spread information operations to combat, deter and influence adversaries.

SCEIIO During Political Tensions - Election Periods

39. A second type of context in which SCEIIOs are employed are during periods of tension between states, i.e. in the grey area between war and peace. In these, SCEIIO campaigns form part of the broader political and diplomatic dynamic and are often intertwined with some more offensive components. With regard to the examples studied, this was notably the case with Russia's influence campaigns during the US and French Presidential elections in 2016 and 2017 respectively. However, these are not the only cases, with relevant literature citing a large number of others, for example in the recent British, Finnish, German, Austrian and Dutch elections to name only a few (Baezner, 2017). On the US side, in contrast, there appear to be few or even no open sources identifying similar cyber-enabled campaigns during foreign elections, despite a long list of historical precedents of foreign election intervention, with the US having intervened in 81 elections around the world between 1946 and 2000. However, if one had to make an educated guess, it could be safely assumed that such activities would not have stopped suddenly at the turn of the millennium once the digital age had arrived.

40. With regard to the two cases examined, a number of observations can be made. First, the level of technical sophistication of the cyberattacks against the Democratic National Convention (DNC) and the Clinton and Macron campaigns is consistently at the medium end. While it is known that APT28 has used some

moderately sophisticated malware (i.e. X-agent) to infiltrate, remain hidden, and exfiltrate data, there is no evidence that the attack resulting in the Macron leaks unfolded in the same way. As such, these hacks, and the subsequent doxing, are the only recorded (and attributed) types of SCEITOs in terms of election meddling. Indeed, while some DDoS attacks (using the Mirai botnet) and website defacements were mentioned in the news, notably against Trump's and Clinton's campaign websites, these have not been traced back to any Russian operations. This absence of DDoS could be due to the inherently covert nature of cyber influence campaigns, which is in conflict with the high visibility of DDoS attacks and defacements and shines a spotlight on the victim's vulnerabilities. More importantly, though, these types of attacks would have diverted public attention and media resources from other divisive issues that were being pushed via social media influence operations for example.

41. In addition to these attacks, there have been reports of sophisticated hacks of electoral materials in the US, where specifically the voting systems of 39 states were hit. In some cases the attackers gained access to voter data, which they tried to alter and delete. In other cases they accessed campaign finance databases. A second case was also observed in Ukraine in 2014, where CyberBerkut hacked its way into the Ukrainian Central Election Commission and changed the election results to portray the ultra-right candidate Dmytro Yarosh as the winner. While the operations were averted in both cases, *in extremis* in the Ukrainian case, the operations were effective even without altering voting outcomes. In fact, efforts to delete voter registration information or slow down election counts were made in order to undermine confidence in election processes and institutions.

42. With regard to SCEIIOs, the use of the full spectrum of tools and techniques has been identified in both cases, from mass disinformation on social media amplified by bots, to sockpuppets and Kremlin-affiliated news alongside trolling and flaming. The two cases also present similar objectives and targets, tailored to each context, which include polarization, disruption, undermining trust, controlling narratives, supporting specific candidates, among others. The short timespan of only a few months that separated these elections was most likely the reason why no new techniques were deployed. However, there was a notable difference in the scale, reach and efforts – but not impacts – of these two operations. Indeed, according to a report on the Internet Research Agency (DiResta et al., 2018), the scale of their operations in America was unprecedented, reaching over 126 million people on Facebook, 20 million users on Instagram, and 1.4 million on Twitter, while uploading over 1000 videos on YouTube. The same report estimates the cost of this campaign to have been at least US$25 million. No definitive estimate has been made of the costs of interfering in the French elections, but it is suspected to be less. It is worth mentioning that the EU and France took a number of measures to mitigate foreign influence operations in the wake of the US elections. These included the following, among others: awareness-raising workshops for candidates; a ban on Russian TV outlets; pressure on Facebook to close automated accounts; the planting of fake documents to confuse hackers; and the abandonment of electronic voting for citizens living abroad (Baezner, 2017). Another difference can be seen in the reliance on domestic actors for trolling and disinformation. In the French case, a number of far-right groups not only reused Russian propaganda and contents but also exchanged know-how and materials with similar groups abroad (Baezner, 2017).

SCEIIOs During Political Tensions: Non-Election Periods

43. SCEIIOs have been used in non-election periods, for example in Estonia in 2007 and in Turkey between 2015 and 2016. Similar to election meddling, these cyber influence campaigns again form part of broader political and diplomatic efforts. In Estonia, the campaign was linked to Russia's energy diplomacy and agenda in Northern Europe, while in Turkey it was associated with Russia's involvement and interests in the Syrian civil war. A comparison identifies clear differences between the two cases in terms of targets, tools and objectives, which arise due to the very different contexts in which the campaigns were conducted.

44. The operations in Turkey, for instance, involved mostly SCEIIOs amplified via social media, ranging from disinformation (e.g. anti-American conspiracy theories or false authorship) to narrative laundering by so-called experts in addition to trolling and flaming. As such, they were focused on reinforcing narratives, undermining NATO, and fomenting distrust and uncertainty against institutions and allies (Costello, 2018). The level of sophistication was low, and operations were mostly operated by proxies. In the Estonian case, in contrast, which happened before the widespread use of social media, SCEIIOs were largely technical in nature. They included mostly unsophisticated tools (i.e. DDoS and defacement) deployed by a criminal network with links to the Kremlin to disrupt day-to-day life in Estonia (i.e. government, finance, media), instil a sense of insecurity, and undermine trust in Estonian institutions. In addition, these attacks aimed at influencing politicians to consider Russian views and therefore resembled earlier (Soviet-era) destabilization

and deterrence tactics towards governments deemed insufficiently friendly or compliant.

Democratic Versus Authoritarian Regimes

45. From a more general perspective, it is interesting to discuss the broader use, scope and types of cyber influence operations used by two different types of regimes, i.e. a liberal democracy (such as the US) and an autocratic state (such as Russia). It must, however, be noted that the extent to which relevant observations can be generalized to apply to other democratic and autocratic regimes though relevant, cannot be extrapolated in totality.

46. **Democratic Regimes**.

(a) In liberal democratic regimes, SCEIIOs are highly normalized but constrained within a relatively narrow operational scope at all times, whether during peace, war or political tensions. They are strictly prohibited – or extensively limited – in times of peace, though. **In addition, the use of propaganda by the government or state agencies against their own population or that of a friendly foreign state has traditionally been frowned upon and deemed unacceptable by the general public.** The rules of engagement are thus highly codified and controlled by domestic laws, such as the US Smith-Mundt Act, which prohibits any form of influence operations by the Pentagon against US citizens and news outlets. Democratic governments are generally committed to adhering to the rule of law, laws of governmental responsibility and the principle of freedom of speech. They thus remain accountable to their population and sensitive to popular outrage, which can have repercussions in later elections.

(b) Nonetheless, this does not mean that SCEIIOs are not taking place in one form or another. However, they are conducted in a more transparent fashion and not labelled as such, with white propaganda, for example, having been adapted to modern information technologies. Today, all governments not only release most of their official statements online but also engage with and operate actively on social media to diffuse their own narrative. This is not only done on behalf of entities such as the US Department of State but also by and through top-level bureaucrats such as the President or Secretary of State, among others, and a network of individuals who amplify official messages (e.g. through retweets). Public diplomacy as well as public and civilian affairs are other domains which use cyberspace to "win the population's hearts and minds". Both aim at achieving popular support, whether abroad during military deployments or at home to foster support and understanding for current engagements.

(c) Meanwhile, SCEIIOs against enemies are both allowed and tolerated in liberal regimes but only at certain times (i.e. during conflicts or war) and within a limited geographical scope (i.e. within the battlespace). Moreover, their use is restricted to furthering strategic and tactical objectives rather than pursuing economic interests. These operations thus remain highly controlled within their doctrinal framework. Both the scope and use of information operations are codified and limited to the military and its agents with the support of the intelligence agencies, while foreign services conduct public diplomacy. The approach to IOs is highly compartmentalized.

(d) Furthermore, in the current age of interconnectedness, even authorized cyber influence campaigns against hostile populations during times of war pose an issue for a democratic regime's domestic population. As became evident in 2002 in the context of Rumsfeld's controversial *Office for Strategic Influence* activities, there is nothing to stop US individuals or media from picking up, further disseminating or being affected by online propaganda, whether grey or black, or disinformation aimed at foreign populations (Carver, 2002). This has regularly led the public and regulators to demand more transparency, particularly in the wake of Snowden's revelations about mass internet surveillance by the US.The contentious case of Rumsfeld's office and the political backlash that led to its dissolution highlight another feature of democratic regimes, namely the existence of checks and balances and corrective mechanisms to any (perceived) abuses of the normative framework pertaining to the use of SCEIIOs.

(e) Overall, while state-led SCEIIOs are highly normalized, there tends to be greater tolerance for non-state-driven cyber influence, especially in the fields of politics and business. Indeed, there are now a plethora of companies promoting and selling their marketing, advertising, brand management, and public relations services to politicians, celebrities and other companies. These services provided include a number that verge on a legal grey area, such as buying likes or subscribers or exploiting legal psychographic data (i.e. Cambridge Analytica) for political targeting. Influence has become a commonly traded good, with many actors trying to get a slice of the pie and exploiting one technique or another. A perfect example of this type of

commercialized online influence are social media influencers, i.e. individuals who, through their online presence on various social media such as Twitter, Facebook, or Instagram, have a critical mass of followers replicating the fashions, locations or attitudes (e.g. clothing, makeup, restaurants) promoted by these online personalities and their sponsors.

47. **Authoritarian Regimes**.

(a) In contrast to democratic regimes, SCEIIOs in authoritarian regimes are not bound by the same norms and restrictions. Influence operations against domestic targets are considered not only acceptable by such regimes but also necessary to maintain the desired degree of social control over the population. In Russia, this was particularly notable during the anti-government and election protests in 2011–2012 (the Snow Revolution). During that time, Russia refined its SCEIIOs to dominate, monitor and suppress online debate as well as divert the use of social media for facilitating organization. It developed increasingly sophisticated social media techniques, including sophisticated trolling and DDoS attacks on news websites, fake hashtag and Twitter campaigns (using bots), and social media operations closely coordinated with campaigns conducted in other media (Helmus , 2018). However, Russia is by no means the only state to use such techniques against its own population, with other examples including China and North Korea. All of these actors manipulate media without restraint, aided by the relative homogeneity and stability of their leaderships, which greatly assists the dissemination of a singular message and narrative while allowing sufficient operational flexibility (Cohen & Bar'el, 2017).

(b) Furthermore, such internal/domestic influence can be seen to spill over into external influence. Indeed, most of the SCEIIO techniques – particularly those pertaining to social media – were first refined and tested domestically before being used for propaganda or disruption purposes abroad. This applies particularly to various Russian-speaking communities outside Russia, for example in eastern Ukraine, which were specifically targeted by pro-Russian propaganda through Russian media and social media (such as VKontakt) in the wake of the Ukrainian conflict.

(c) Moreover, unlike democratic nations, authoritarian states are not organized around the distinction between war and peace in their laws, regulations and societal institutions. This is particularly true for those who uphold a narrative of continuous struggle with another entity. Such a stance allows authoritarian states to develop institutions and competencies that are much more closely integrated at the operational level and navigate between different levels of tension with relative authority and ease, particularly around the level of low-intensity warfare just below the threshold of war (Lin & Kerr, 2019). As a result, while SCEIIOs are also based on and regulated by doctrine, this doctrine is very different from the liberal democratic one. For example, Russia's very broad and holistic understanding of IW allows a much broader use and scope of relevant capabilities. The range of SCEIIOs/SCEITOs used is extensive and even includes highly sophisticated cyberattacks against voting systems and critical infrastructures, both of which are strictly off-limits for democracies.

(d) Lastly, authoritarian regimes are, again due to their organizations and institutions, both less vulnerable to SCEIIOs and better equipped to respond to them than democracies. Indeed, as mentioned earlier, they are more flexible operationally, less restricted normatively, and have a greater scope of use but, above all, their exposure to potential attacks is smaller than in democracies. Indeed, democratic states' respect of the rule of law and freedom of speech, as well as the open and public nature of democratic societies (e.g. in terms of media etc.) and their election processes make them particularly vulnerable targets for SCEIIOs.

Trends of Election Related SCEIIOs

48. ASPI's International Cyber Policy Centre (Sarah O'Connor et al, 2020) has identified 41 elections and seven referendums between January 2010 and October 2020 that have been subject to cyber-enabled foreign interference in the form of cyber operations, online information operations or a combination of the two. **Figure 3.3** shows that reports of the use of cyber-enabled techniques to interfere in foreign elections and referendums has increased significantly over the past five years. Thirty-eight of the 41 elections in which foreign interference was identified, and six of the referendums, occurred between 2015 and 2020 (Figure 3.3). These figures are significant when we consider that elections take place only every couple of years and that referendums are typically held on an *ad hoc* basis, meaning that foreign state actors have limited opportunities to carry out this type of interference. As a key feature of cyber-enabled interference is deniability, there are likely many more cases that remain publicly undetected or unattributed. Moreover, what might be perceived as a drop in recorded cases in 2020 can be attributed to a number of factors, including

election delays caused by Covid-19 and that election interference is often identified and reported on only after an election period is over.

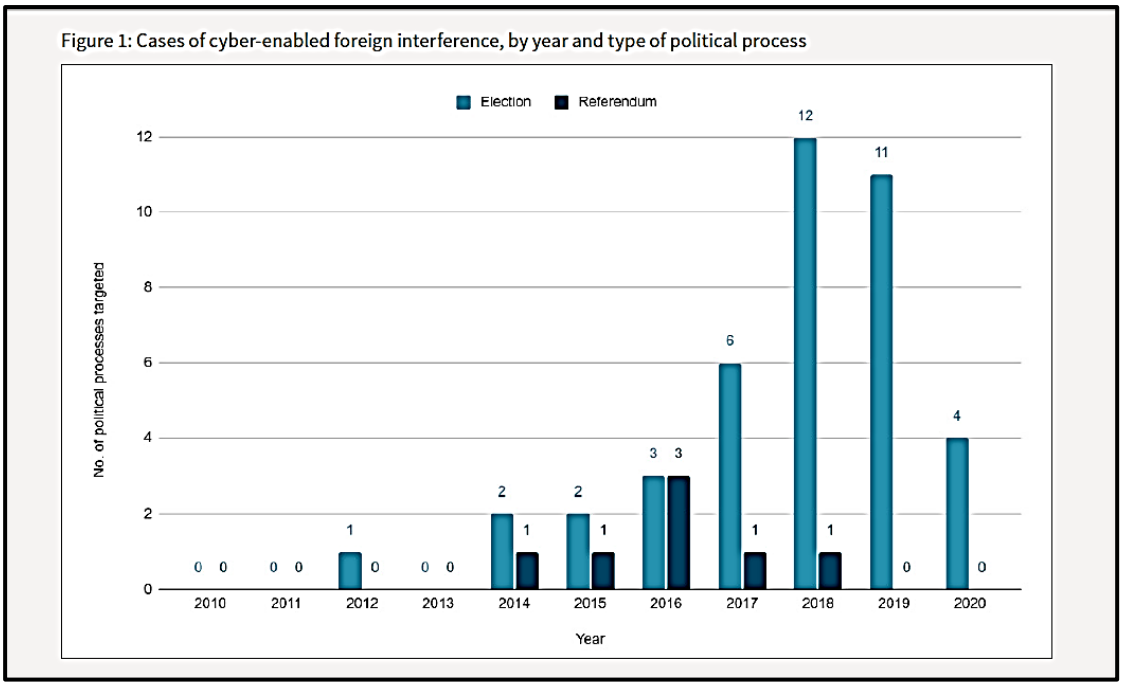


Figure 3.3 – Cyber Enabled Foreign Interference by Year & Type of Political Process

49. Cyber-enabled interference occurred on six continents (Africa, Asia, Europe, North America, Australia and South America) - **Figure 3.4**.The research (**Figure 3.5**) identified 33 states that have experienced cyber-enabled foreign interference in at least one election cycle or referendum, the overwhelming majority of which are Democracies. The EU has also been a target: several member states were targeted in the lead-up to the 2019 European Parliament election. India is conspicuously untouched.

Figure 2: Targets of cyber-enabled foreign interference in an election or referendum

Note: The numbers in the map represent the number of reported cases of cyber-enabled foreign interference in an election or referendum. Access this interactive map here. Source: Maptive, map data © 2020 Google.

Figure 3.4– Targets of SCEIIO in Election or Referendum

Figure 3: Number of political processes targeted (1–4), by state or region

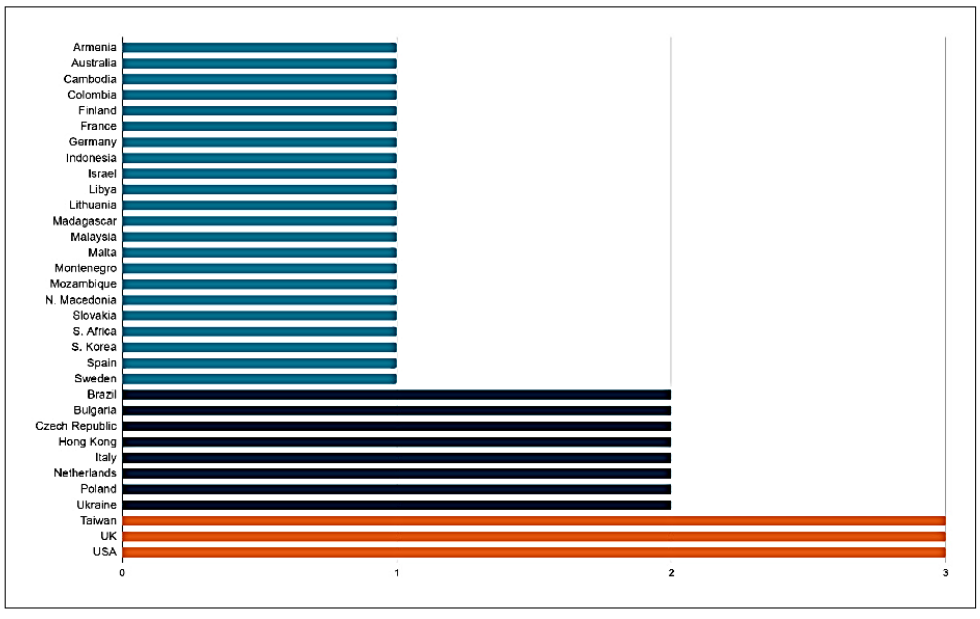


Figure 3.5 – No of Pol Processes Targeted(1-4), By State Or Region

50. **SCEITO**. This research identified 25 elections and one referendum over the past decade in which SCEITO were used for interference purposes. In the context of election interference, cyber operations fell into two broad classes: operations to directly disrupt (such as DoS attacks) or operations to gain unauthorised access (such

as phishing). Unauthorised access could be used to enable subsequent disruption or to gather intelligence that could then enable online information operations, such as a hack-and-leak campaign. Phishing attacks were the main technique used to gain unauthorised access to the personal online accounts and computer systems of individuals and organisations involved in managing and running election campaigns or infrastructure. They were used in 17 of the 25 elections, as well as the referendum, with political campaigns on the receiving end in most of the reported instances. Phishing involves misleading a target into downloading malware or disclosing personal information, such as login credentials, by sending a malicious link or file in an otherwise seemingly innocuous email.

51. **SCEIIO**. This research identified 28 elections and six referendums over the past decade in which SCEIIOs were used for interference purposes. In the context of election interference, SCEIIO should be understood as the actions taken online by foreign state actors to distort political sentiment in an election to achieve a strategic or geopolitical outcome. They can be difficult to distinguish from everyday online interactions and often seek to exploit existing divisions and tensions within the targeted society. SCEIIO combine social media manipulation ('inauthentic coordinated behaviour'), for example partisan media coverage and disinformation to distort political sentiment during an election and, more broadly, to alter the information environment. The operations are designed to target voters directly and often make use of social media and networking platforms to interact in real time and assimilate more readily with their targets. SCEIIO tend to attract and include domestic actors. There have been several examples in which Russian operatives have successfully infiltrated and influenced legitimate activist groups in the US. This

becomes even more prominent as foreign state actors align their SCEIIO with domestic disinformation and extremist campaigns, amplifying rather than creating disinformation. The strategic use of domestic disinformation means that governments and regulators may find it difficult to target them without also taking a stand against domestic misinformers and groups.

52. **It is important to acknowledge the synergy of the two attack vectors as this synergy would inform any organizational construct that is charted out and also how they can converge and reinforce one another**. The research identified three elections where cyber operations were used to compromise a system and obtain sensitive material, such as emails or documents, which were then strategically disclosed online and amplified. For example, according to *Reuters*, classified documents titled 'UK-US Trade & Investment Working Group Full Readout' were distributed online before the 2019 British general election as part of a Russian-backed strategic disclosure campaign. The main concern with the strategic use of both attack vectors is that it further complicates the target's ability to detect, attribute and respond. This means that any meaningful response will need to consider both potential attack vectors when securing vulnerabilities.

53. Significantly, this research identified 11 states that were targeted in more than one election cycle or referendum (**Figure 3.4**). The repeated targeting of certain states is indicative of their (perceived) strategic value, the existence of candidates that are aligned with the foreign state actors' interests, insufficient deterrence efforts, or past efforts that have delivered results. This research also identified five cases in which multiple foreign state actors targeted the same election or referendum (the 2014 Scottish independence referendum, the 2016 UK referendum on EU membership, the

2018 Macedonian referendum, the 2019 Indonesian general election and the 2020 US presidential election). Rather than suggesting coordinated action, the targeting of a single election or referendum by multiple foreign state actors more likely reflects the strategic importance of the outcome to multiple states.

54. **Attack Vectors** The attack vectors are SCEITO(Cyber Operations) and SCEIIO (Online Information Operations). Of the 48 political processes targeted, 26 were subjected to SCEITO and 34 were subjected to SCEIIO. Twelve were subjected to a combination of both (**Figure 3.6**).

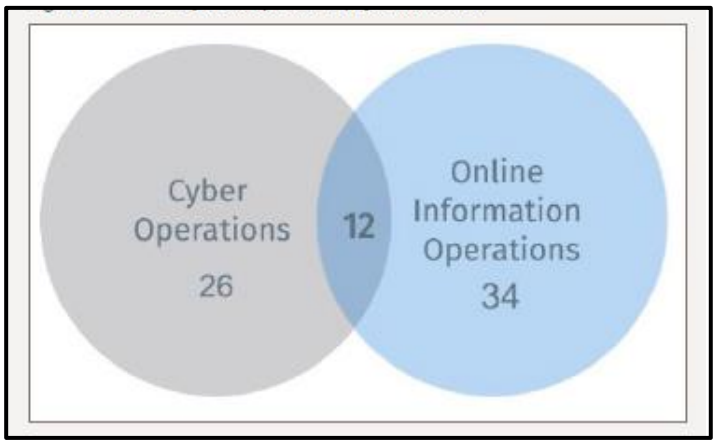


Figure 3.6 – Attacks on Political Processes by Attack Vectors

State Actors And Targets

55. Cyber-enabled foreign interference in elections and referendums between 2010 and 2020 has been publicly attributed to only a small number of states: Russia, China, Iran and North Korea. In most cases, a clear geopolitical link between the source of interference and the target can be identified; Russia, China, Iran and North Korea mainly target states in their respective regions, or states they regard as adversaries— such as the US. The increasing cohesion among foreign state actors, notably China and Iran learning and adopting various techniques from Russia, has made it increasingly difficult to distinguish between the different foreign state actors.

This has been further complicated by the adoption of Russian tactics and techniques by domestic groups, in particular groups aligned with the far-right.

56. **Russia**. Russia is the most prolific foreign actor in this space. The ASPI research identified 31 elections and seven referendums involving 26 states (**Figure 3.7**) over the past decade in which Russia allegedly used cyber-enabled foreign interference tactics. Unlike the actions of many of the other state actors profiled here, Russia's approach has been global and wide-ranging. Many of Russia's efforts remain focused on Europe, where Moscow allegedly used cyber-enabled means to interfere in 20 elections, including the 2019 European Parliament election and seven referendums. Of the 16 European states affected, 12 are members of the EU and 13 are members of NATO. Another focus for Russia has been the US and while the actual impact on voters remains debatable, Russian interference has become an expected part of US elections. Moscow has also sought to interfere in the elections of several countries in South America and Africa, possibly in an attempt to undermine democratisation efforts and influence their foreign policy orientations. Russia appears to be motivated by the intent to signal its capacity to respond to perceived foreign interference in its internal affairs and anti-Russian sentiment. It also seeks to strengthen its regional power by weakening alliances that pose a threat. For instance, Russia used SCEITO and SCEIIO to interfere in both the 2016 Montenegrin parliamentary election and the 2018 Macedonian referendum. This campaign was part of its broader political strategy to block the two states from joining NATO and prevent the expansion of Western influence into the Balkan peninsula.

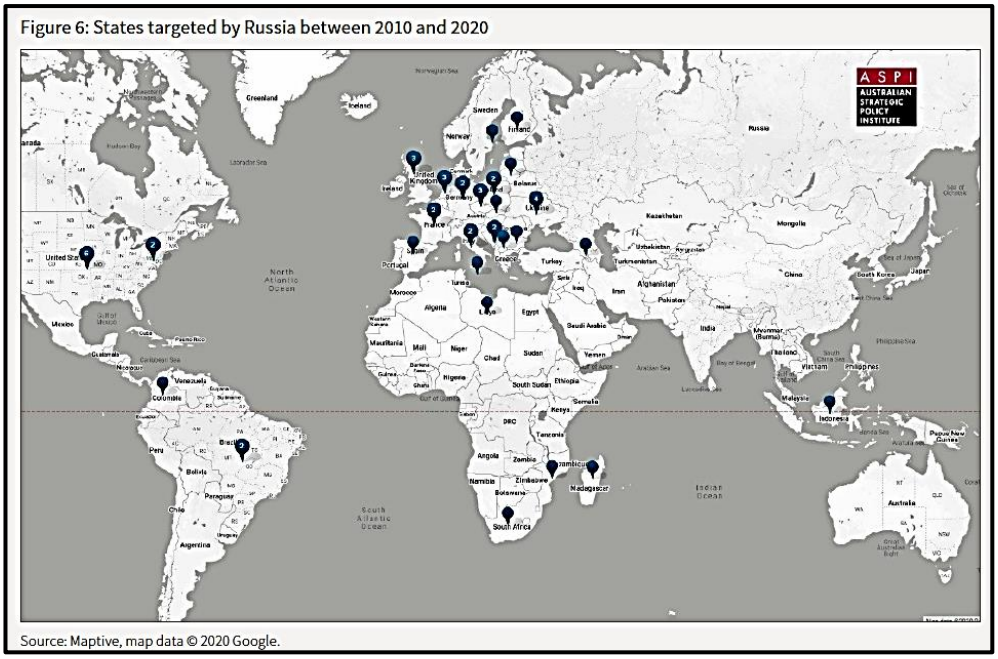


Figure 3.7 – States Targeted by Russia – 2010 to 2020

57. **<u>China</u>** Over the past decade, it's been reported that China has targeted 10 elections in seven states and regions (**Figure 3.8**). Taiwan, specifically Taiwanese President Tsai Ing-wen and her Democratic Progressive Party, has been the main target of China's cyber-enabled election interference. Over the past three years, however, the Chinese state has expanded its efforts across the Indo-Pacific region. Beijing has also been linked to activity during the 2020 US presidential election. As reported by the *New York Times* and confirmed by both Google and Microsoft, state-backed hackers from China allegedly conducted unsuccessful spear-phishing attacks to gain access to the personal email accounts of campaign staff members working for the Democratic Party candidate Joseph Biden. China's interference in foreign elections is part of its broader strategy to defend its 'core' national interests, both domestically and regionally, and apply pressure to political figures who challenge those interests. Those core interests, as defined by the Chinese Communist Party, include the preservation of domestic stability, economic development, territorial

integrity and the advancement of China's great-power status. Previously, China's approach could be contrasted with Russia's in that China attempted to deflect negativity and shape foreign perceptions to bolster its legitimacy, whereas Russia sought to destabilise the information environment, disrupt societies and weaken the target. More recently, however, China has adopted methods associated with Russian interference, such as blatantly destabilising the general information environment in targeted countries with obvious mistruths and conspiracy theories.

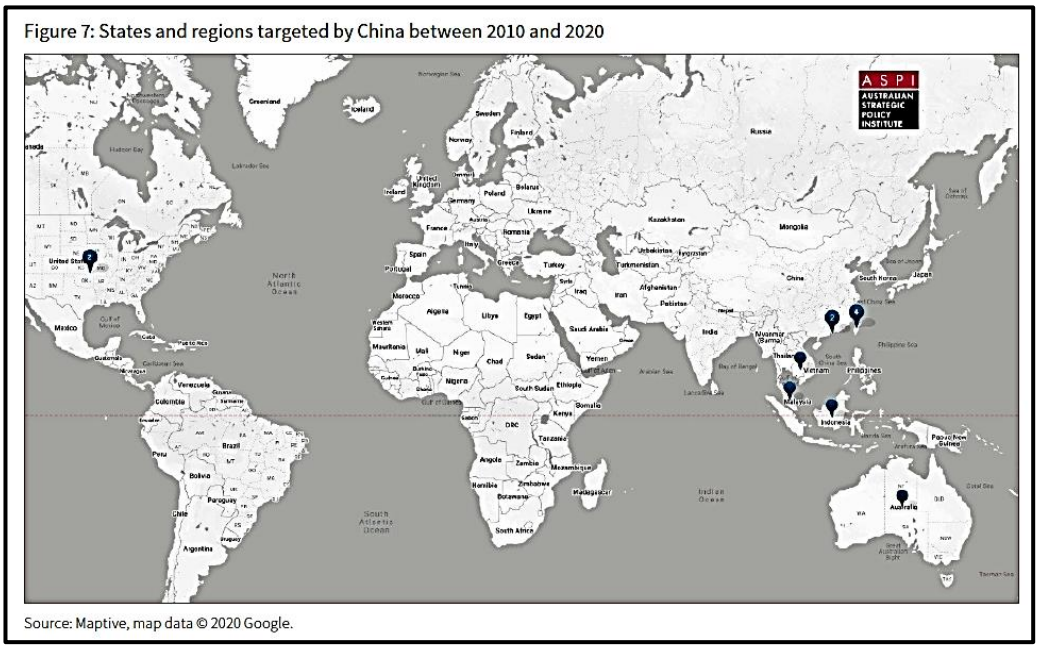


Figure 3.8 – States & Regions Targeted by China between 2010 & 2020

58. **Iran**. This ASPI report shows that Iran engaged in alleged interference in two elections and two referendums in three states (**Figure 3.9**). Iranian interference in foreign elections appears to be similar to Russian interference in that it's a defensive action against the target for meddling in Iran's internal affairs and a reaction to perceived anti-Iran sentiment. A pertinent and current example of this is Iran's recent efforts to interfere in the 2020 US presidential election by targeting President Trump's campaign. As reported by the *Washington Post*, Microsoft discovered that the Iranian-backed hacker group Phosphorus had used phishing emails to target 241 email

accounts belonging to government officials, journalists, prominent Iranian citizens and staff associated with Trump's election campaign and successfully compromised four of those accounts.

Figure 3.9 – States Targeted by Iran Between 2010 & 2020

59. **<u>North Korea</u>**. North Korea has been identified as a foreign threat actor behind activity targeting both the 2020 South Korean legislative election and the 2020 US presidential election – **Figure 3.10**. Somewhat similarly to China's approach, North Korea's interference appears to focus on silencing critics and discrediting narratives that undermine its national interests. For example, North Korea targeted North Korean citizens running in South Korea's 2020 legislative election, including Thae Yong-ho, the former North Korean Deputy Ambassador to the UK and one of the highest-ranking North Korean officials to ever defect.

Figure 9: States targeted by North Korea between 2010 and 2020

Source: Maptive, map data © 2020 Google.

Figure 3.10 – States Targeted by North Korea Between 2010 & 2020

Detection and Attribution

60. Detection and attribution requires considerable time and resources, as those tasks require the technical ability to analyse and reverse engineer a SCEITO or SCEIIO. Beyond attribution, understanding the strategic and geopolitical aims of each event is challenging and time-consuming. The covert and online nature of cyber-enabled interference, whether carried out as a SCEITO or an SCEIIO, inevitably complicates the detection and identification of interference. For example, a DoS attack can be difficult to distinguish from a legitimate rise in online traffic. Moreover, the nature of the digital infrastructure and the online information environment used to carry out interference enables foreign state actors to conceal or falsify their identities, locations, time zones and languages.

61. As detection and attribution capabilities improve, the tactics and techniques used by foreign states will adapt accordingly, further complicating efforts to detect

and attribute interference promptly. There are already examples of foreign state actors adapting their techniques, such as using closed groups and encrypted communication platforms (such as WhatsApp, Telegram and LINE) to spread disinformation or using artificial intelligence to generate false content.65 It can also be difficult to determine whether an individual or group is acting on its own or on behalf of a state. This is further complicated by the use of non-state actors, such as hackers-for-hire, consultancy firms and unwitting individuals, as proxies.

62. Ahead of the 2017 Catalan independence referendum, for example, the Russian-backed media outlets *RT* and *Sputnik* used Venezuelan and Chavista-linked social media accounts as part of an amplification campaign. The hashtag #VenezuelaSalutesCatalonia was amplified by the accounts to give the impression that Venezuela supported Catalonian independence. More recently, Russia outsourced part of its 2020 US presidential disinformation campaign to Ghanaian and Nigerian nationals who were employed to generate content and disseminate it on social media.

Global Landscape of Disinformation (SCEIIO) or Computational Propaganda

63. The manipulation of public opinion over social media remains a critical threat to democracy. **Industrialized Disinformation : 2020 Global Inventory of Organised Social Media Manipulation , a report by Oxford University** (Samantha Bradshaw et al, 2021) has, over the past four years, monitored the global organization of social media manipulation by governments and political parties, and the various private companies and other organizations they work with to spread disinformation.

The 2020 report highlights the recent trends of computational propaganda across 81 countries and the evolving tools, capacities, strategies, and resources used to

manipulate public opinion around the globe. Three key trends have been identified in this 2020 inventory of disinformation activity as follows:-

(a) Disinformation activity continues to increase around the world. This year, evidence of 81 countries using social media to spread computational propaganda and disinformation about politics was found. This has increased from last years' report, in which 70 countries with disinformation activity were identified.

(b) Over the last year, social media firms have taken important steps to combat the misuse of their platforms by disinformation propagators. Public announcements by Facebook and Twitter between January 2019 and November 2020 reveal that more than 317,000 accounts and pages have been removed by the platforms. Nonetheless, almost US $10 million has still been spent on political advertisements by disinformationists operating around the world.

(c) Private firms increasingly provide manipulation campaigns. In 2020 report, firms operating in forty-eight countries, deploying computational propaganda on behalf of a political actor were discovered. Since 2018 there have been more than 65 firms offering computational propaganda as a service. In total, almost US $60 million was spent on hiring these firms since 2009.

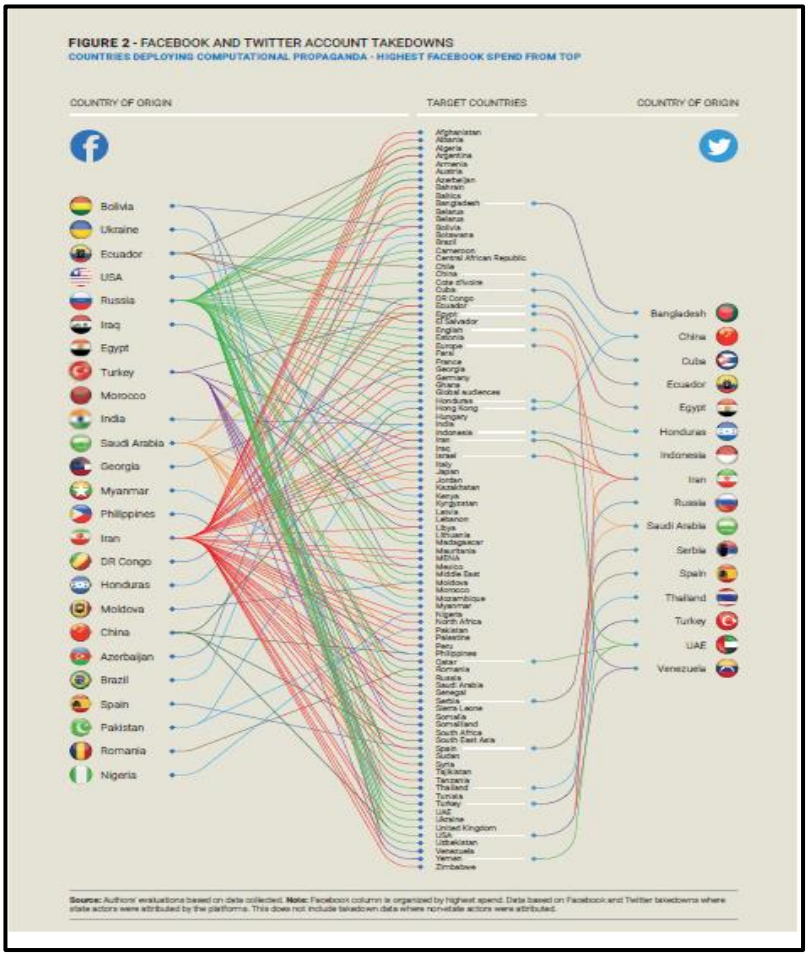


Figure 3.11 – Facebook & Twitter Account Takedowns

64. **Figure 3.11** gives out the Facebook and twitter account takedown country-wise as well as the target countries. India, very clearly has not engaged in any disinformation activity globally. China, Russia & Iran appear to be the largest perpetrators in terms of number of targets however the highest Facebook spend for deploying computational propaganda is of Bolivia with USA at fourth place.

Figure 3.12 – Organizational Form & Prevalence of Social Media Manipulation

TABLE 1 - ORGANIZATIONAL FORM AND PREVALENCE OF SOCIAL MEDIA MANIPULATION

Country	Government Agencies	Politicians & Parties	Private Contractors	Civil Society Organizations	Citizens and Influencers
Angola	■	■	■		
Argentina	■	■	■		
Armenia	■	■	■	■	
Australia	■	■			■
Austria		■			
Azerbaijan	■	■		■	■
Bahrain	■		■		■
Belarus	■			■	■
Bolivia	■		■		■
Bosnia & Herzegovina	■			■	■
Brazil	■	■	■		■
Cambodia	■	■			■
China	■		■	■	■
Colombia	■	■	■		
Costa Rica		■	■	■	■
Croatia	■	■			
Cuba	■				■
Czech Republic		■			■
Ecuador	■	■	■		
Egypt	■	■	■		
El Salvador	■	■	■		■
Eritrea	■				
Ethiopia	■	■			■
Georgia	■	■	■		
Germany		■			■
Ghana	■	■			■
Greece	■	■			■
Guatemala	■	■	■		■
Honduras	■		■		■
Hungary	■	■	■		■
India	■	■	■		■
Indonesia		■	■	■	■
Iran	■	■		■	
Iraq	■	■	■	■	
Israel	■	■	■	■	■
Italy		■	■		
Kazakhstan	■	■	■	■	
Kenya	■	■	■		■
Kyrgyzstan	■	■			■
Kuwait	■	■	■	■	■
Lebanon		■	■		
Libya	■	■	■	■	■
Macedonia		■			■
Malaysia	■	■	■	■	■
Malta	■	■	■		
Mexico	■	■	■		
Moldova		■			■
Myanmar	■				
Netherlands		■			
Nigeria		■	■		■
North Korea	■			■	
Oman	■				
Pakistan	■	■			
Philippines	■	■	■	■	■
Poland	■	■	■	■	■
Qatar	■		■		
Russia	■	■	■	■	■
Rwanda	■	■	■		■
Saudi Arabia	■	■	■		■
Serbia		■			■
South Africa	■	■	■		■
South Korea	■	■			■
Spain		■	■		■
Sri Lanka		■			
Sudan	■	■			■
Sweden		■			
Syria	■		■	■	
Taiwan		■	■	■	■
Tajikistan	■			■	
Thailand	■				■
Tunisia	■	■	■		
Turkey	■	■	■		■
Ukraine		■	■		■
United Arab Emirates	■		■		■
United Kingdom	■	■	■	■	■
United States	■	■	■	■	■
Uzbekistan	■				■
Venezuela	■	■	■		■
Vietnam	■		■		■
Yemen	■	■			
Zimbabwe	■	■			■

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of political actors using social media influence operations, and where examples of those organizations found. For Government Agencies, Political Parties, Private Contractors, Civil Society Organizations and Citizens and Influencers. ■ = Organizations found □ = No evidence found.

65. **Figure 3.12** gives out the organizational form and social media manipulation in various countries. USA, UK, Russia, Kuwait, Poland, Philippines, Malaysia & Libya have all organizational forms deploying computational propaganda. Iran does not employ private contractors and China does not have politicians or Political parties employing it, obviously due to a single party system. In India, civil society and organizations do not appear to be involved.

Figure 3.13 – Fake Account Types

TABLE 2 - FAKE ACCOUNT TYPES

Country	Bots	Human	Hacked or Stolen
Angola	●	●	
Argentina	●	●	
Armenia	●	●	
Australia	●	●	
Austria		●	
Azerbaijan	●	●	●
Bahrain	●	●	
Belarus		●	
Bolivia	●	●	
Bosnia & Herzegovina		●	
Brazil	●	●	
Cambodia	●	●	
China	●	●	
Colombia	●	●	
Costa Rica		●	
Croatia		●	
Cuba	●	●	●
Czech Republic		●	
Ecuador	●	●	●
Egypt	●	●	●
El Salvador	●	●	
Eritrea		●	
Ethiopia		●	●
Georgia	●	●	
Germany	●	●	
Ghana		●	
Greece	●	●	
Guatemala	●	●	●
Honduras	●	●	
Hungary		●	
India	●	●	
Indonesia	●	●	
Iran	●	●	●
Iraq		●	
Israel	●	●	
Italy	●	●	
Kazakhstan		●	
Kenya	●	●	
Kyrgyzstan		●	
Kuwait	●	●	
Lebanon	●	●	

Country	Bots	Human	Hacked or Stolen
Libya	●	●	
Macedonia	●	●	
Malaysia	●	●	
Malta		●	
Mexico	●	●	
Moldova	●	●	
Myanmar	●	●	
Netherlands		●	
Nigeria	●	●	
North Korea		●	●
Oman	●	●	
Pakistan	●	●	
Philippines	●	●	
Poland	●	●	
Qatar	●	●	
Russia	●	●	●
Rwanda		●	
Saudi Arabia	●	●	●
Serbia		●	●
South Africa	●	●	●
South Korea	●	●	
Spain	●	●	
Sri Lanka	●	●	
Sudan		●	
Sweden	●	●	
Syria	●	●	
Taiwan	●	●	
Tajikistan		●	
Thailand	●	●	
Tunisia		●	
Turkey	●	●	●
Ukraine	●	●	
United Arab Emirates	●	●	●
United Kingdom	●	●	
United States	●	●	
Uzbekistan		●	
Venezuela	●	●	
Vietnam	●	●	
Yemen	●	●	
Zimbabwe		●	

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of fake accounts identified between 2010-2020. Bots refer to highly-automated accounts. For fake social media account types: ● = Automated Accounts, ● = Human Accounts, ● = Hacked, Stolen or Impersonation Accounts, ● ● ● = No evidence found.

66. In **Figure 3.13**, the breakdown on types of fake accounts reveals that mostly authoritarian sates deploy all three forms viz Bots, Humans & Hacked /Stolen accounts. The differentiator between authoritarian and democratic states is the hacked/stolen accounts.

67. The report stratifies countries into High, Medium & Low Capacity in terms of ability and resources to deploy computational propaganda (**Figure 3.14**). Interestingly, India is bracketed along with USA, UK, Russia, China and Pakistan as "High Capacity". The same however is not reflected in any national structures or organizational coordination. Possibly, few agencies may be undertaking this activity to counter local disinformation rather than an organized strategic construct based on a plan/strategy to counter adversary disinformation and employ SCEIIO as a tool of achieving national security objectives.

Figure 3.14 – Capacity of States for Disinformation

TABLE 5 - CYBER TROOP CAPACITY

HIGH CAPACITY

Country	Recent Activity	Status	Coordinated Cybertroop Team	Resources Spent	Coordination
China	✓	Permanent	✓	✓	Centralised
Egypt	✓	Permanent		✓	Decentralised
India	✓	Permanent	✓	✓	Centralized
Iran	✓	Permanent		✓	Centralised
Iraq	✓	Permanent	✓	✓	Somewhat Centralised
Israel	✓	Permanent	✓	✓	Centralised
Myanmar	✓	Permanent	✓	✓	Centralized
Pakistan	✓	Permanent	✓	✓	Decentralised
Philippines	✓	Permanent	✓	✓	Centralized
Russia	✓	Permanent	✓	✓	Centralized
Saudi Arabia	✓	Permanent	✓	✓	Centralised
Ukraine	✓	Permanent		✓	Centralized
United Arab Emirates	✓	Permanent	✓	✓	Centralised
United Kingdom	✓	Permanent	✓	✓	Decentralised
United States	✓	Permanent	✓	✓	Decentralised
Venezuela	✓	Permanent	✓	✓	Centralized
Vietnam	✓	Permanent	✓	✓	Somewhat Centralised

CHAPTER IV : ORGANIZATIONAL STRUCTURES FOR SCEIIO : MAJOR GLOBAL PLAYERS

"In the age of social media, the idea that history is written by the victors was an old fashioned notion. History was being written in the moment in 140 characters. What was new was that our adversaries were writing the history before the battle, shaping the victory narrative before there was a victory."

- ***General John Allen, Special Presidential Envoy, Coalition to Counter ISIS***

" Attacking an adversary's most important centre of gravity – the spirit of its people – no longer requires massive bombing runs or reams of propaganda. All it takes is a smartphone and a few idle seconds….They might even divide and conquer a nation's politics from afar."

- ***Emerson T Brooking- Likewar***

1. The design framework of organizational structures for SCEIIO of major global players is centred around the nature of the state i.e. Authoritarian or Democratic and the consequent operating concept of SCEIIO follows suit. This of course is informed by the traditional doctrinal moorings of these states concerning Political Warfare, Propaganda and Information Operations. Hence the Chinese and Russian structures would be vastly centralised and have diffused structures to avoid attribution while the Western construct was more limited to only military operations by Defence Forces. Organizations created within civilian administrative structures were mostly defending against disinformation. A holistic addressal of the SCEIIO paradigm with a designated lead agency is absent. Meanwhile there were civil society and multination initiatives again mostly looking at Defence against SCEIIO, both the "Supply and

Demand Sides". Many recommendations address the "supply side" of disinformation (Alina Polyakova & Daniel Fried, 2019) i.e. they recommended, and continue to recommend, policies and actions to limit the influx of disinformation into democracies and other media ecosystems. But, tools to block disinformation will be imperfect, and some degree of disinformation will be part of the media landscape for the indefinite future. Addressing the "demand side" of disinformation—i.e. reducing general social acceptance of fabrications and distortions—is likely to be more important for sustained societal immunity. It is critical that governments, social media companies, and civil-society groups invest in long-term resilience against disinformation, including raising social awareness of disinformation and encouraging digital literacy education, including how to discern fabricated or deceptive content and sources.

Framing Solutions Against a Moving Target

2. Russia was perhaps first among major powers to deploy techniques of full-spectrum, state-sponsored disinformation for the digital age—the intentional spread of inaccurate information designed to influence societies and it will not be the last. Other state actors with perhaps greater capabilities, such as China, and non state actors, such as terrorist groups with a higher tolerance for risk, will adapt the disinformation toolkit to undermine democracies or are already doing so. There is nothing new about state propaganda and other means of political subversion ("active measures" was the term of art for Soviet efforts of this kind). But, digital and social media, in combination with more traditional methods, offer new means to achieve traditional ends. Russia's democratic and pro-Western neighbours, especially Ukraine, Georgia, and the Baltic states, have contended with Russian disinformation attacks for years.

Other targets of state-sponsored disinformation campaigns—the United States and some Western European countries—woke up late to the challenge, with the United States doing so only after its 2016 presidential election, in which Russia played a large and malign role. The Department of Justice Special Counsel Report and two independent reports, prepared for the US Senate's Select Committee on Intelligence and published in December 2018, detail Russia's disinformation tactics during and after the 2016 US elections, including by the Russian-government-supported Internet Research Agency (IRA), the now-notorious St. Petersburg troll farm. The February 2018 Department of Justice indictment of thirteen Russian operatives involved in the IRA information operations provides the most in-depth research to date about the internal machinery of the Russian operation.

3. Hence, Disinformation campaigns are not going away. Quite the opposite—other malicious state actors with an interest in undermining democracies, including Iran, North Korea, and China, are learning from Russian tactics. Meanwhile, the tools of attack are evolving and adapting to democratic responses. State-sponsored disinformation campaigns aim to amplify existing social divisions and further polarize democratic societies. As such, they don't stop when the ballot box closes. Still, due to the high level of attention and consequential outcomes, elections provide an ideal high-impact opportunity for this type of influence operation. Ahead of elections throughout Europe and North America in 2019 and 2020, governments, social media companies, and civil-society groups must learn from each other and accelerate the implementation of best practices to defend against disinformation. Democracies are learning that means of defence and norms of resilience applicable to traditional propaganda and subversion are inadequate to meet the present danger. Also, disinformation techniques will continue to evolve. For example, innovation in artificial intelligence

(AI) is producing “deepfakes” and other “synthetic media” products—video and audio manipulation with the capability to manufacture the appearance of reality, such as non existent, but real-looking, remarks by a political leader. As these tools become more low cost and accessible, they will become perfect weapons for information warfare. More generally, disinformation techniques are shifting from the use of simple automated bots to more sophisticated interaction with (and manipulation of) domestic groups, extremist and otherwise, through various forms of impersonation and amplification of organic posts by domestic actors. Thus, it may be increasingly difficult to disentangle foreign-origin disinformation from domestic social media conversations. Rather than trying to break through the noise, the new strategy aims to blend in with the noise—obfuscating manipulative activity and blurring the line between authentic and inauthentic content. **Hence, the need for intense inter agency coordination to ensure synergy between organizations addressing domestic and foreign disinformation is essential.**

USA

4. As cyberspace presents an easy, cost-effective method to communicate a message to large swathes of populations, much of present day information warfare takes place on the internet, leading some to conflate “cyber warfare” with information warfare. While IO in the United States tends to be seen as a purely military activity, other countries and terrorist organizations have robust information warfare strategies and use a whole-of-government or whole-of-society approach to information operations. In terms of U.S. government bureaucracy, there are debates in the United States about where the IW centre of gravity should be. During the Cold War, the epicentre in the U.S. government was the Department of State and the U.S.

Information Agency. Since 9/11, much of the current doctrine and capability resides with the military, leading some to posit that the epicentre should be the Pentagon. But others worry that the military should not be involved in the production of propaganda.

5. Although several official documents now refer to “information warfare” in other countries, the United States has no formal government definition of IW. The DOD definition of information operations refers only to military operations and does not emphasize the use of cyberspace to achieve non military strategic objectives. Similarly, there is no commonly accepted definition of “cyber warfare”; rather, the military refers to offensive and defensive cyberspace operations, with cyberspace as a warfighting domain or operating environment. Cyberspace operations differ from information operations, which are specifically concerned with the use of information-related capabilities, such as military information support operations or military deception. Cyber-enabled information operations can be characterized as IO conducted in cyberspace. Just as IO carries its own doctrine and associated organizational structures, so do cyberspace operations, which are generally considered the purview of the United States Cyber Command. The U.S. Cyber Command is building a national cyber mission force composed of three teams, one of which assists combatant commanders in the field with planning and operations. These teams may, for example, target and dismantle violent extremist websites that present an operational threat to troops on the ground. However, this cyber force is structurally and conceptually separated from the troops responsible for conducting information operations. As previously stated, the two forces operate under separate doctrine. The two are physically separated as well: U.S. Cyber Command is located in Fort Meade,

MD, while the Joint Information Operations Warfare Center is located at Lackland Air Force Base, Texas (Catherine A. Theohary, 2018).

6. As a source of national power, information is a critical strategic asset, and currently the information element is shared within the U.S. government. During the Cold War, the U.S. Information Agency (USIA) was responsible for supporting U.S. national interests abroad through information dissemination. It was later folded into the State Department's Bureau of Public Diplomacy and Public Affairs before being disbanded in 1999. Today, the Department of State-led interagency Global Engagement Center (GEC) is charged with many of the former USIA activities. According to Steve Goldstein, then Undersecretary for Public Diplomacy, the GEC recently launched a new $40 million initiative to battle state-sponsored disinformation and propaganda targeting the United States and its interests. It also plans to launch a series of pilot projects with the Department of Defense, using additional DOD funding. Within the U.S. government, much of the current information warfare doctrine and capability resides with the military, making it the de facto centre of gravity. DOD is also relatively well-funded, leading some to posit that the epicentre for IW activities should be the Pentagon. Some fear that military leadership of the IW sphere represents the militarization of cyberspace, or the weaponization of information that would counter the principles of global internet freedom. Title 10 U.S.C 2241 prohibits DOD from domestic "publicity or propaganda," although the terms are undefined. It is unclear how IW/IO relate to this so-called military propaganda ban. The Central Intelligence Agency (CIA) has a history of conducting information warfare or psychological operations, particularly with respect to countering guerilla organizations abroad. Monitoring Soviet disinformation was once

solely the purview of the CIA, until the Active Measures Working Group was established in 1981 and tasked with coordinating the activities of multiple, disparate activities within the U.S. government.

7. During the Cold War, the Interagency Active Measures Working Group collected and analyzed information gathered at USIA overseas posts, from CIA reporting, and FBI investigations in order to detect and expose Soviet propaganda and disinformation efforts. This information was published in publicly disseminated reports. The final report of the Active Measures Working Group in 1992 warned that with the dissolution of the Soviet Union, active measures remained a threat to U.S. interests: "As long as states and groups interested in manipulating world opinion, limiting U.S. government actions, or generating opposition to U.S. policies and interests continue to use these techniques, there will be a need for the United States Information Agency to systematically monitor, analyze, and counter them."24 Because there is no similar entity existing today, some government analysts have suggested that a version of the Active Measures Working Group be convened to face the current threat environment. Similarly, there have been calls for the resurrection of the U.S. Information Agency, but with added responsibilities.

8. Some policymakers have questioned whether tampering with, interfering with, or otherwise influencing a sovereign nation's democratic processes in an IW campaign is an act of war that could trigger a military response. A similar question is whether a cyberattack that falls below the threshold of damage and destruction resulting from a kinetic event could be considered an armed attack or use of force under international law, or whether data breaches of military networks or theft of sensitive defense information constitute an act of aggression rather than espionage.

There are questions over whether the United States has a strategy in place to match the robust IW strategies of its competitors, and whether the U.S. government has institutions, organization, and programs to wage and win an information war or to deter foreign information operations. **With respect to cyberspace and information operations, the structures supporting each set of capabilities are currently bifurcated within the Department of Defense**. In addition, cyberspace operations tend to focus on computer network attacks rather than the cognitive and strategic effects of information. Again, it is moot whether current organizational and doctrinal constructs support the full integration of these capabilities to maximize their effects, and whether ongoing conceptual confusion has inhibited DOD's ability to respond to IW challenges. When responding to foreign IW activities on the United States, Congress may consider whether authorities are in place for DOD to conduct counter-IO, and if other interagency entities are authorized and resourced to conduct coordinated efforts. Another consideration may be the efficacy of IW as a military function or a whole-of-government responsibility (Catherine A. Theohary, 2018).

9. More recently, there have been isolated attempts within the U.S. Defense Department to posture organizational resources to fight effectively in the information domain. For example, in the global conflict against the Islamic State, one combatant command implemented a reorganization to integrate and synchronize lethal and non-lethal effects, notably by aligning Information Related Capabilities (IRCs) previously located and managed by leaders in their J2, J3, and J6 offices under a single advocate for information operations in the operations division (J3). A senior defense official noted, "We must be organized properly" to be effective at information operations. This example shows that organization was the solution to harmonize the effects of

multiple strategic communication tools found in otherwise disjointed and stove-piped IRCs. The British, Soviet experiences, and the Islamic State example illustrate that strategic information operations are more successful when an organization dedicated to information related activities, both offensive and defensive, is responsible for management and oversight of the operations. The World War II and Cold War examples show that when centrally managed, information operations inform and shape specific audience perceptions in order to gain a competitive advantage. The United States presently lacks a unified framework to identify, defend, counter, integrate, and synchronize its available information capabilities for multi domain operations, and it should consider a new organizational construct to address these challenges in the future (Ben Hatch, 2019).

10. The 2018 NDAA directs the Secretary of Defense to designate a senior official responsible for multi-domain strategic information operations. Further, it directs the creation of a "cross-functional task force to integrate DoD organizations responsible for information operations, military deception, public affairs, electronic warfare, and cyber operations." According to Dr. Christopher Paul, "It seems self-evident that if we are to avoid information fratricide, we need to be coordinating all the messages and signals." The office's primary responsibility would be to produce strategy, conduct planning, and champion a budget meant to "counter, deter, and conduct strategic information operations and cyber-enabled information operations." The office would be responsible for determining what information to disseminate to a given audience, and what information to protect from disclosure. Establishing the office would clarify roles and responsibilities, and reduce bureaucracy by implementing an integrated

structure for offensive and defensive information operations that can move at the speed of our adversaries.

11. There are two cogent options under the current defense structure to consider for implementation of the NDAA direction. The first is to align information responsibilities to the Under Secretary of Defense for Intelligence (USD(I)). Information operations, however, are military operations and require intelligence support, but they are not directly intelligence operations. While OUSD(I) could assume a greater role, it does not appear to be the most appropriate office for information operations. Alternatively, the Office of the Under Secretary of Defense for Policy (USD(P)) could assume these new responsibilities. On face value, this would be a logical placement as current policy assigns responsibility to the OUSD(P) for oversight of information operations in the DoD, and USD(P) acts as the principal staff advisor to the Secretary of Defense for information. History suggests, however, there are disadvantages to a more robust OUSD(P) role (Ben Hatch, 2019).

12. A previous attempt to align strategic information operations under OUSD(P) ended with great controversy. In 2001, OSD created the Office of Strategic Influence and it reported directly to the USD(P). Although originally focused on defense issues linked to constructing strategy and objectives targeting specific audiences, OSD envisioned the Office would eventually become an established interagency organization with the charter to conduct strategic influence campaigns. However, someone with knowledge of the office and its mission leaked information to the media suggesting the Office would seed foreign media with misinformation and false

messages. Public uproar ensued, and as a result, then Secretary Rumsfeld closed the office.

13. The controversy could recur if there was a repeat of the initiative. In her 2003 Army War College article, LTC Susan Gough interviewed a senior official with knowledge of OUSD(P) inner dynamics. She quotes the senior official as stating there remained fears that "whoever sabotaged [the Office of Strategic Influence]" will sabotage future efforts as well. Although this incident occurred in 2001, senior leaders would need to evaluate the risk of a greater OUSD(P) role for information operations. Ultimately, revisiting the approach of reassigning strategic information operations to OUSD(P) may have a similar outcome as experienced in 2001. Additionally, there are challenges with the current construct of aligning information operations under either OUSD(I) or OUSD(P) during a crisis. According to LTG P.K. Keen, a key observation from Joint Task Force (JTF)-Haiti was the need to communicate with a multitude of audiences in one voice. To assist in this effort, the JTF established a Joint Information and Interagency Center (JIIC), an organizational construct LTG Keen recommended be codified for future JTFs. Within the JIIC, there would be a team dedicated to social media, blogs, websites, and other resources, such as public affairs media professionals, ready to advance the strategic narrative and counter any misinformation through cyber-enabled information operations. Further, the center would serve as a centralized information coordination and synchronization hub for all messaging and information sharing from the tactical to strategic levels (Ben Hatch, 2019).

14. More senior defense leaders believe that centralized organization matters for how to conduct information operations in the future and are making changes. The

Secretary of Defense assigned the U.S. Special Operations Command (USSOCOM) as the Joint Proponent for Military Information Support Operations (MISO), and directed USSOCOM to establish a centralized DoD MISO Global Messaging/Counter Messaging capability, with $1.8 million allocated in FY 2019 for the initiative.50 Further, LTG Stephen Fogarty, U.S. Army Cyber Commander, said the Army is moving towards merging its cyber and electronic warfare functional areas. LTG Fogarty believes, "It's time to think seriously about absorbing other historically-distinct mission areas – or tribes – including information operations." Another option available consistent with LTG Fogarty's August 2019 announcement to absorb information operations into U.S. Army Cyber Command, and change its name to the Army Information Warfare Command, is the potential for U.S. Cyber Command (USCYBERCOM) to assume responsibility as global synchronizer for United States strategic information operations and cyber-enabled information options. Moreover, USCYBERCOM could restructure into an Information Warfare Command similar to the Army model. USCYBERCOM hosted a panel that considered this option. An October 2018 USCYBERCOM Cyber Strategy Symposium highlighted the ongoing challenges experienced by the current practice of subdividing information operations and cyberspace capabilities, however, the proposed solutions focused on what USCYBERCOM could do to augment the nation's ability to conduct strategic influence operations rather than moving to oversee these operations. While USCYBERCOM is postured to deliver operationalized information or defend against an adversary's information attacks in cyberspace, the multi domain nature of the mission and associated requirements for the information enterprise appear to align more with NDAA direction to assign these responsibilities to a senior official at the undersecretary of defense level.

15. Presently, the USA has the following agencies/initiatives dealing with SCEIIO/Disinformation (Alina Polyakova & Daniel Fried, 2019):-

(a) **US Executive**. The following are active :-

(i) **Global Engagement Center (GEC)**. A State Department unit within the Public Diplomacy Bureau, initially intended to focus on countering extremist Islamist ideology, has turned to countering state-sponsored disinformation, with an appropriated budget of $120 million. The GEC has begun to disperse significant funding to civil society groups and private-sector partners, including: for research into disinformation and counter-disinformation tactics ($9 million); to journalists, fact checkers, and online influencers ($9 million); to partner organizations to support local counter-disinformation efforts; and to develop new technologies useful for counter-disinformation actions. The GEC is also actively participating in the G7 RRM, the UK-US bilateral coalition, and the Australian-led counter-interference effort.

(ii) **Department of Defense**. Funds the GEC (mandated under a National Defense Authorization Act). Beyond the traditional strategic communications functions conducted by its public-affairs apparatus, the Defense Department's policy arm has a narrow mandate to direct information support activities under the Special Operations/Low Intensity Conflict (SO/LIC) unit, typically in support of US military activities overseas or relations with allies and partners. US European Command (EUCOM) supports the broader US effort to counter Russia's

disinformation and conducts information operations as part of its foreign-presence exercises in Europe, e.g., in Poland.

(iii) **FBI.** The mandate of the Federal Bureau of Investigation's (FBI) Foreign Interference Task Force (FITF), established in October 2017, includes engagement with US technology and social media companies to address the challenge of false personas and fabricated stories on social media platforms (as well as "hard" cybersecurity for voting infrastructure and other potential US election-related targets). At least one social media company has credited the FITF with advancing US government (USG)-social media company discussions to address the threat.

(iv) **US Cyber Command**. Began operations ahead of the 2018 congressional elections, to deter Russian operatives from potential interference. Cyber Command has reportedly sent messages to specific individuals active in disinformation operations, de facto outing them and their activities.

(v) **Department of Homeland Security (DHS)**. Has an internal working group focused on countering malign influence, but its activities seem more focused on technical election security around critical infrastructure than on broader disinformation.

(vi) **US State Department's Bureau for European and Eurasian Affairs**. Has established a new position— the senior adviser for Russian malign activities and trends (SARMAT)—tasked with coordinating policy on Russian malign influence.

(vii) **State Department With Like-Minded European Governments**.State Department has worked with like-minded European governments to establish an informal consultative group on disinformation efforts.

(viii) **USG Interagency Working Group—The Russian Influence Group (RIG)**. Includes the relevant US government agencies, including DHS, the intelligence community, the State Department, and the Department of Defense. However,no USG senior official has been empowered to take the lead on counter-disinformation efforts. Policy issues without senior-level ownership tend to drift.

(ix) **Department of the Treasury**. Used existing authorities to impose sanctions on Russian entities tied to disinformation efforts, including those directed at the 2016 US presidential election. This included the sanctions designation on December 19, 2019, of entities and individuals tied to the IRA and nine GRU (military intelligence) officers. Material accompanying the Treasury Department's sanctions designations exposed details of Russian operation, including establishment of an online English-language website, "USA Really."

(b) **US Congress**. Following agencies /initiatives are current :-

(i) The 2019 National Defense Authorization Act (NDAA) added significant (albeit second-order) provisions defining the importance of countering disinformation for US national security.

(ii) Cementing the role of the GEC by defining its counter-disinformation task within the parameters of US national security, likely securing the centre's longer-term funding in future iterations of the NDAA.

(iii) Defining "malign influence" as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, business, corruption, educational, and other capabilities by hostile foreign powers to foster attitudes, behaviours, decisions, or outcomes within the United States."

(iv) Authorizing the establishment of a new position in the National Security Council (NSC) responsible for coordinating the interagency process for countering foreign malign influence. This NSC director-level position now exists and was filled at the time of this writing.

(v) The Honest Ads Act, introduced in October 2017 and likely to be reintroduced in the current Congress, would require that political ads be identified as such on social media platforms. On one level, the legislation would address only a small number of online ads (those strictly defined as sponsored by a political candidate or campaign). But, by making social media companies liable should they provide a platform for foreign expenditures aimed at influencing US elections (already prohibited under US campaign-finance law), the Honest Ads Act could conceivably curtail Russian-placed and other foreign-placed issue ads with a partisan purpose, including ads placed under hidden or misleading sponsorship. In any case, the legislation has not moved through either chamber of Congress.

Possibly to preempt legislation, both Twitter and Facebook have announced that they are implementing many Honest Ads Act requirements. The impact of these announcements is not yet clear and would be limited if these social media companies apply the Act's definitions narrowly. Even if Congress were to pass this legislation, its impact may not be great. Political ads make up a miniscule portion of the overall ads industry. In addition, ads are a secondary tool for spreading disinformation; organic posts, albeit under false identities, are becoming the major Russian disinformation tool.

(vi) The Senate Special Committee on Intelligence (SSCI) commissioned two major reports on the IRA's tactics and techniques, based on data shared by Twitter, Facebook, and Google.

(vii) The Senate introduced the Data Protection Act of 2018, which would have placed standards on what online service providers can do with end-user data. While the bill has not been reintroduced in the new Congress, it laid out the responsibilities of providers in handling user data, and it enjoyed wide support from platforms.

(viii) The Senate has reintroduced the Defending American Security from Kremlin Aggression Act of 2019 (DASKA); while mostly devoted to sanctions, it also "calls for the establishment of a National Fusion Center to Respond to Hybrid Threats, a Countering Russian Influence Fund to be used in countries vulnerable to Russian malign influence, and closer coordination with allies"

(ix) In April 2019, Senators Mark Warner (D-VA) and Deb Fischer (R-NE) introduced the Deceptive Experiences to Online Users Reduction (DETOUR) Act, which seeks to limit tactics used by social media platforms to steer users in various directions. DETOUR appears directed against domestic deceptive online practices, not foreign disinformation. But, the bill suggests that Congress is moving beyond pushing transparency (as in the Honest Ads bill) and toward introduction of more intrusive standards of conduct for social media companies. The precedent could provide a basis for legislation targeting disinformation.

(x) Congress's main activity on countering disinformation has been to hold hearings with social media companies and their executives. Since 2016, the US Congress has held five open hearings with Google, Facebook, and Twitter executives. These have captured intense media attention and may have generated political pressure on the social media companies to be seen as constructive with respect to disinformation issues. Congress has not, however, decided what specific steps it wants the social media companies to take to address issues of data privacy, online advertising transparency, algorithmic transparency with respect to placement of news, or more transparency on how the companies are identifying or de-prioritizing/de-ranking disinformation campaigns, or removing them from their platform.

Russia

16. The use of the term Information Warfare in American public discourse to describe Russia's interference in the internal political affairs of other countries is

problematic. Like other terms, such as Hybrid Warfare, Information Warfare has no doctrinal definition and is correspondingly ambiguous. Its meaning is further diluted or outright misused by practitioners at the operational level in fields that would be better considered as subsets of the term information warfare. The general notion of information warfare as a "strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations" as described by the Congressional Research Service (CRS), is often used liberally to describe narrower activities, such as network operations, psychological operations, electronic warfare, operations security, and military deception. This conflict is in part due to the operationalization of Information Warfare in the United States, which is bound by the confines of legal and cultural barriers. In practice, "much of the current information warfare doctrine and capability resides with the military." However, the U.S. military's doctrine, capabilities, and functions (Information Operations) do not address the strategic level, but rather the operational and tactical ones. In addition, as the report of the CRS points out, Title 10 U.S.C. § 2241 prohibits the Department of Defense (DOD) from domestic "publicity or propaganda." Although the U.S. military is expected to be involved in Information Warfare, there are barriers to its ability to influence beyond the operational level of war. At the same time, there seems to be no other institution in the U.S. government entrusted with a role in Information Warfare at the strategic level (Blagovest Tashev et al, 2019).

17. It has been pointed out by others that the U.S. military used to have a more comprehensive and holistic approach to information warfare and at some points even involved coordination and synchronization of policies and actions by military and non-military agencies and structures. Gradually, however, the various information-

related functions and organizations went in different directions. Very importantly, information warfare was increasingly associated with the military and warfighting, divorcing it from any broader—civilian, non-military and peacetime—efforts in the information environment. This is a critical point, as the discussion below will indicate that Russia not only faces fewer legal and cultural barriers to influence at the operational and strategic level during both war and peace, but it also has philosophically different approaches and goals while operating in the information environment. The multiple issues with the definition of Information Warfare in the United States notwithstanding, even the most expansive understanding of the term fails to capture the nature of the approach adopted by Russia. As Timothy Thomas (Timothy L. Thomas, 2020) observed, what is really different in the Russian approach "is the conceptual understanding of an information operation from a cultural, ideological, historical, scientific, and philosophical viewpoint." The distinct nature of Russia's approach is so different from the American approach that many argue for adopting a new term that better captures Russia's way and avoids mixing it with the Western conceptualization of operations in the information environment. One author, for example, calls for adopting IPb, a shorthand for the Russian term информационное противоборство, loosely meaning "information confrontation."

18. **Russia's Elevation of Information Warfare**. Through its strategic documents, Russia consistently indicates that it seeks to adopt a comprehensive and coordinated approach to gaining security and successfully advancing its interests through the Information Environment (Blagovest Tashev et al, 2019) :-

(a) This effort is envisioned as the integration of multiple instruments of power and the involvement of both national institutions and nongovernmental actors. In fact, the body of strategies, doctrines, and government-promoted narratives suggests that the successful promotion of Russia's national interests requires the involvement of the entire society. Russia has also increasingly placed emphasis on non-military means as a way to gain security, even as the country is involved in an ambitious military modernization. According to General Valery V. Gerasimov, chief of the General Staff of the Armed Forces of the Russian Federation, the ratio of non - military to military measures in the modern security environment is 4:1, even as non-military competition comes under the aegis of the military. To the best of our knowledge, this is the only reference Gerasimov, or any other high-ranking Russian military official, has made to this ratio. One can reasonably suspect that the chief of the General Staff is paying lip service to the increasingly large role non-military measures are playing in confrontations between states; the Russian military elite is still focused on preparing the armed forces to prevail in a kinetic confrontation with other states. There is little doubt, however, that the Russian military recognizes the utility of non-military measures in interstate confrontation, especially during what would be considered peacetime.

(b) This way of thinking is leading to an evolution in the Russian way of warfare; while the military is not necessarily departing from the big-war paradigm, decision makers in Moscow are increasingly focusing on how defence structure and posture, along with non-military instruments, shape the strategic environment in line with Russia's preferences. Accordingly,

information warfare is increasingly central to a state's arsenal to use against other states in confrontation, wherein countries' elites and public perceptions are becoming the centre of gravity in determining confrontation outcomes. The goal of information warfare is to influence both the adversary's strategic calculus and the public's behaviour. As Aleksander Dvornikov, commander of Russia's Southern Military District, points out in the Russian publication *Military-Industrial Courier*, "Now states achieve their geopolitical goals through the application of complex non-military measures, which often are more effective than the military ones. The main goal of these measures is not the physical destruction of the enemy but the complete submission of his will." He goes on to argue that without information operations, Russia would not have succeeded in many operations in Syria.

(c) Not surprisingly, Russia is implementing policies and practices designed to promote information warfare to a level of parity with nuclear and conventional power. This struggle to shape other states' perceptions and calculus is constant, even during peacetime and periods of cooperation; thus, the lines between peace, conflict, and war are blurred. As General Gerasimov puts it, "military conflicts have not gone beyond the bounds of the conventional nature of war; their components are types of struggle such as direct armed struggle, political struggle, diplomatic struggle, information struggle, et al." While the U.S. approach to warfare, largely conditioned by political and legal constraints, makes a relatively clear distinction between war and peace and restricts methods and capabilities accordingly, Russian thinking displays a willingness to harness the power of all national institutions in a

continuous struggle with its opponents, both current and potential. Ironically, Russian strategists see the elevation of informational instruments of influence, the blurring of the line between peace and war, and even hybrid warfare as innovations advanced and practiced by Western powers. Hence, Russia is simply adapting to the new type of warfare. While the enemy's economy and state command and control system will continue to be priority targets, the information sphere becomes a new critical operating environment.

(d) The growing popularity of terms such as hybrid war, political warfare, and gray zone conflict emanating from the West point out attempts to rationalize what is seen as a new type of confrontation between states. Russia, conversely, has long seen relations between states as inherently and constantly competitive. Russia's attention to changing trends in the information environment is reflected in official security-related documents. The Russian 2015 National Security Strategy (NSS) identifies informational security as one of the components of national security along with the state, public, environmental, economic, transportation, energy, and individual components. The Russian NSS goes on to point out that the United States and its allies are attempting to contain Russia by exerting political, economic, military, and informational pressure on it.

(e) In general, Russia sees an intensifying confrontation in the global information arena as some states (meaning the West) use information and communication to achieve their geopolitical objectives. Russia's NSS is specifically concerned with Western attempts to use information as a tool to interfere in Russia's domestic affairs to weaken "traditional Russian spiritual

and moral values" and to threaten the "unity of the Russian Federation's multinational people." Likewise, *The Foreign Policy Concept of the Russian Federation* pledges to respond to these challenges by continuing to focus on traditional measures to ensure strategic deterrence. Internally, the state also tasks itself with implementing policies "aimed at strengthening and augmenting traditional Russian spiritual and moral values," in other words, creating resilience against foreign cultural influences. This focus on traditional Russian values is not new. In a wide-ranging series of interviews in 2000, when asked what the country needed most, then-acting President Vladimir Putin responded, "moral values."

19. **Context and Aims of Alleged Russian Propaganda**. Moscow blends attributed, affiliated, and non-attributed elements and exploits new realities of online and social media to conduct information warfare at a perhaps unprecedented scale and level of complexity. These information operations, which recall the Soviet-era "active measures," appear to be a growing priority within the Kremlin :-

(a) The Kremlin's social media campaigns cannot be entirely separated from its information operations involving traditional media, because traditional news stories are now crafted and disseminated online. Moreover, the Kremlin's narrative spin extends far beyond its network of media outlets and social media trolls; it is echoed and reinforced through constellations of "civil society" organizations, political parties, churches, and other actors. Moscow leverages think tanks, human rights groups, election observers, Eurasianist integration groups, and orthodox groups. A collection of Russian civil society organizations, such as the Federal Agency for the Commonwealth

of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation, together receive at least US$100 million per year, in addition to government-organized nongovernmental organizations (NGOs), at least 150 of which are funded by Russian presidential grants totaling US$70 million per year.

(b) In some parts of Moldova, local public channels charge for EU advertisements while airing, for free, the advertisements of the League of Russian Youth and Motherland—Eurasian Union, an organization whose Christian activism is infused with Russian politics (see Lough et al., 2014). In the Baltic states of Latvia, Lithuania, and Estonia, Russia's narrative is fortified in media through such outlets as the First Baltic Channel; in politics via political parties, such as the pro-Russia Latvian Harmony Centre; and, in civil society, by NGOs, such as Native Language, an organization that pushed for making Russian an official language in Latvia in 2012 (see Wilson,2015; see also Auers, 2015).

(c) Russian propaganda also blends and balances multiple aims within a set of information operations. Keir Giles at Chatham House has pointed out more broadly that Russian propaganda aims to pollute the information environment in order to influence what information is available to policymakers or affects them via democratic pressures or to erode trust in institutions, such as host governments and traditional media, often by proliferating multiple false narratives. Andrew Wilson at the Aspen Institute divides Russia's outward-facing propaganda into three categories. The first is

intended to induce paralysis through propaganda. The second seeks to target entities that already have entrenched worldviews with anti-systemic leanings and nudge them in useful directions. The third attempts to fashion alternative realities in which a particular media narrative is reinforced by a supporting cast of pro-Kremlin political parties, NGOs, churches, and other organizations.

(d) The Russian government's sphere of influence is global; it conducts these multifaceted propaganda campaigns in Russian, English, Arabic, French, Czech, Georgian, and a host of other languages. Pomerantsev and Weiss suggest that Moscow's influence can be thought of concentrically: in Ukraine it can create complete havoc; in the Baltic states it can destabilize; in Eastern Europe, co-opt power; in Western Europe, divide and rule; in the US, distract; in the Middle East and South America, fan flames. (Pomerantsev and Weiss, 2014). However, Moscow's reach is most direct in the neighbouring states and former Soviet republics that house sizable ethnic Russian and Russian speaking populations, also called compatriots. The commonality of Russian language provides a springboard for common communication, as well as a potential issue wedge to leverage compatriots against their host countries and governments.

(e) In the Baltic states of Estonia, Latvia, and Lithuania and the east Slavic states Russian-language Kremlin propaganda in these bordering countries draws on aspects of those countries' shared legacy as post-Soviet states. Themes include a common feeling that the West in the late 1990s betrayed them by failing to deliver on promises of prosperity; the supremacy

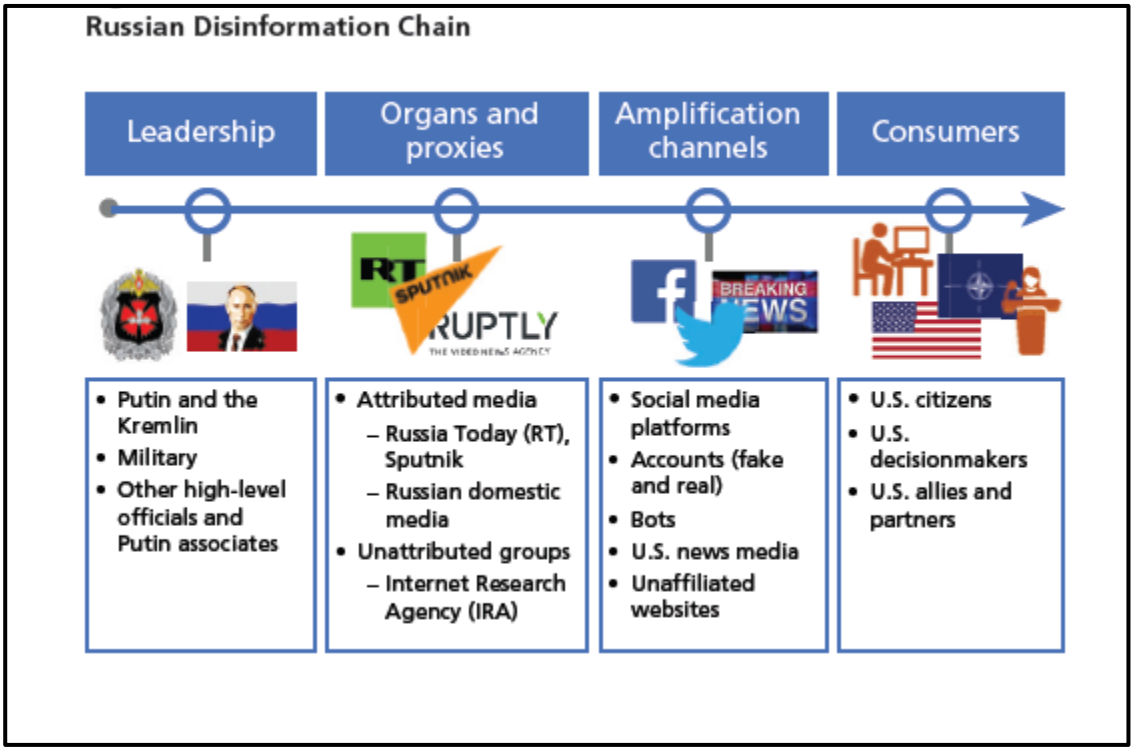
complex of having lost superpower status; the idea that Eurasian civilization is founded on traditional conservative values, such as family and orthodoxy; and, finally, a shared fear of violent revolutions, in which protests are portrayed as slippery slopes to bloody civil wars. Drawing on these shared aspects, the Kremlin can leverage Russian-identifying populations to amplify the Kremlin's message, pressure those populations' host governments, and incite unrest in their host regions or countries. Furthermore, the mere existence of these compatriot populations can be used to legitimize Russia's status as a global leader whose protection is not only needed but welcomed outside of its borders.

(f) In the "far abroad," Russian disinformation seeks to erode trust in institutions. Neil MacFarquhar argued that Russia paints a picture that European government officials are American puppets unable to confront terrorism and the immigration crises (MacFarquhar, 2016). Weisburd, Watts, and Berger divided Russia's aims with propaganda in the "far abroad" into four categories: political, financial, social, and conspiracy. First, they argued that Russian political content aims "to tarnish democratic leaders or undermine institutions" through "allegations of voter fraud, election rigging, and political corruption." Second, the Kremlin's financial messages erode "citizen and investor confidence in foreign markets," positing "the failure of capitalist economies" by "stoking fears over the national debt, attacking institutions such as the Federal Reserve," and attempting to "discredit Western financial experts and business leaders." Third, Russia targets social tensions by emphasizing and leveraging "police brutality, racial tensions, protests, anti-

government standoffs, and alleged government misconduct" in order to "undermine the fabric of society." Finally, conspiracy theories stoke fears of "global calamity while questioning the expertise of anyone who might calm those fears," such as by promoting fears of the U.S. government instituting martial law or nuclear war between Russia and the United States (Weisburd, Watts, and Berger, 2016). The common theme is the goal of creating confusion and undermining trust in Western democratic institutions.

20. **Disinformation Chain**. To analyze the threat posed by Russian disinformation on social media, a framework illustrating the *chain* of Russian influence operations—going from the top leadership to an ordinary consumer in West—from Russian leadership, to organs and proxies of the Russian government, to amplification channels, to consumers, as shown in **Figure 4.1**. This is a very simplified picture of a dynamic, nonlinear process that involves multiple nodes, feedback loops, and other complexities (Elizabeth Bodine-Baron et al, 2018).

Figure 4.1 – Russian Disinformation Chain



(a) **Russian Leadership**. The first step in the chain is the Russian state itself—namely, Russian leadership and the Kremlin. As the Intelligence Community Assessment notes, President Putin "ordered" the influence campaign in the United States. There are questions about how much Russian actors undertaking social media activities are controlled by or coordinated from the top of the Russian government, but it is clear that the influence campaign would not have happened without a high-level decision within Russia's government. Thus, shaping Moscow's decision making offers a key approach to addressing Russian disinformation efforts.

(b) **Organs and Proxies of Russia**. The diverse organizations that actually implement Russia's influence campaign compose the second link in the disinformation chain. Mark Galeotti observed that "Russia's is a broad-based campaign in which the majority of ventures come from the initiative of individuals within and without the government apparatus, guided by their sense of the Kremlin's desires rather than any detailed master plan .Because these entities are so diverse and operate with varying levels of independence from the Russian government, they can be organized into three, potentially four, categories. The first category includes actors who are part of the Russian state, such as the Main Intelligence Unit (GRU) or Sputnik online media. A second category, including entities such as the RT news network, are not formally part of the Russian state but are transparently supported by it. It bears noting that this category includes Americans such as Larry King and

Jesse Ventura, both of whom have programs on RT. A third category involves entities that knowingly act on behalf of the Russian government, but whose connections to the state are concealed, such as the IRA (also known as the "St. Petersburg troll factory"), or webpages that do not have clear Russian attribution, but whose funding connects them to the Russian state. A potential fourth category includes entities that, in effect, act to further the purposes of the Russian government but who are not directly connected to the Russian state. We call those in this category *potential* proxies, because it is debatable whether such actors are proxies in a meaningful sense, and whether direct action to counter them would be feasible or desirable. This includes witting and unwitting participants who are motivated to spread messages convenient to Russia's goals for their own reasons—including those simply holding views the Russian government seeks to promote—and therefore provide an additional channel to achieve Russian goals, such as creating or expanding divisions in American society. This category also includes patriotic Russian hackers and networks run by criminal oligarchs. Different approaches to address the influence of different categories could be needed, given the legal status and position of these actors—some of whom are in Russia and others of whom are based in the United States and Western countries.

(c) **Amplification Channels**. The third link in the chain comprises the various channels (actors and platforms) through which Russian disinformation is intentionally or unintentionally amplified. Social media platforms, such as Facebook and Twitter, play a key amplification role through their policies, algorithms and advertising—a role that can be manipulated, subverted, or

taken advantage of by Russian actors trying to spread disinformation. The accounts that are active on these channels are also particularly important; many play a role in amplifying disinformation, whether they are real or fake, bots, trolls, or regular users. Russian and other foreign contractors who openly offer a variety of social media services for a fee, such as increasing follower counts or posting messages or comments, add an interesting dimension to this link in the chain. Given the variety of openly available Russian social media services, a *plausible* explanation for social media influence campaigns that benefit American interests and that can be traced to Russian accounts is that these campaigns are paid for by U.S. interests and carried out by Russian contractors. An interesting potential example of this kind of social media "service" is when numerous bogus messages appeared on the Federal Communications Commission comment website on the issue of disbanding net neutrality, and the messages turned out to come from Russian sources. As a result, it can be very difficult to link such amplifying channels directly to the Russian state. Finally, western media channels fall into this category, in that they can pick up and spread disinformation.

(d) **Consumers**. The final link in the chain is the set of targets for a given influence campaign. The targets are citizens and decision makers. In other cases, the link might include leaders of North Atlantic Treaty Organization (NATO) allies or other governments, or the populations in NATO countries. This link also overlaps with the amplification channels, in that, in many cases, consumers contribute to the spread of disinformation by posting, retweeting, or otherwise promoting such content. Consumers are particularly important to

highlight, as any effort to lessen the impact of disinformation at this point in the chain must address human nature—changing algorithms or platforms may reduce the visibility of some disinformation, but, in the end, it is up to the user to believe or not believe a particular piece of content Another version from a report published by GEC in 2020 is also shown below.

Figure 4.2 – Pillars of Russia's Disinformation

21. **<u>Major Russian Organisations Effecting SCEIIO</u>**. For Russia, information warfare is a central pillar of the Kremlin's more assertive foreign policy. While propaganda has long been part of the Kremlin's arsenal—playing a prominent role throughout the Cold War—Russia's conflict with Georgia in 2008 marked an important turning point in the Kremlin's use of information warfare. The Kremlin perceived that Russia lost the battle over the narrative of events in Georgia, underscoring for Moscow the importance of being able to advance Russia's worldview. The Russian leadership today views the information domain as one of the fundamental arenas in which states compete. Moreover, Russian leaders do not view their hybrid tactics, including information warfare, as being separate from

conventional military capabilities. Instead, Russia uses information warfare across the full spectrum of conflict and competition between states, including during peacetime. Russia's digital influence operations— part of its information warfare arsenal—seek to shape the attitudes and policy preferences of an adversary's political, military, and civilian populations. Russia uses digital tools to exert influence and change the political dynamics within countries whose policies are contrary to Russian interests. Russian information operations have evolved from the time of the Cold War to capitalize on the contemporary information environment. Russian digital influence activities have proliferated across various ministries and agencies of the government as well as private actors. Some analysts have described the weblike structure of Russian operations, encompassing its intelligence community, Ministry of Defence, Ministry of Foreign Affairs, and proxies such as the Russian Internet Research Agency (IRA), which serves as a primary purveyor of curated content and false information on social media platforms. And while the Russian Presidential Administration (PA) broadly dictates the direction of Russian campaigns based on its priorities and agenda, individual actors within this web have considerable latitude to implement the campaigns as they see fit. In other words, President Vladimir Putin and the PA set the overall direction of Russian digital influence activities, but Russian backed actors often compete to advance these broad directives and have the latitude to act opportunistically and to adapt to local conditions as needed. (Daniel Kliman, et al 2020). It could be said that Russia's capabilities to carry out SCEIIO is distributed primarily amongst three agencies: the Federal Security Service (FSB), the Russian Main Intelligence Directorate (GRU) and a smattering of non-state actors. However, the relative importance of these agencies in the conduct of SCEIIO has varied considerably over time (Lt Gen RS Panwar (Retd), 2021).

(a) **FSB**. In post-Soviet Russia, for a brief period in the 1990s Russia had a separate information security agency, the Federal Agency for Government Communications and Information (FAPSI), which may be considered analogous to the US National Security Agency (NSA). FAPSI was disbanded in 2003, and its components were absorbed largely into the FSB, but also into the Ministry for Internal Affairs of the Russian Federation (MVD RF), the Federal Protective Service of the Russian Federation (FSO RF), and Russia's foreign intelligence service (SVR). The FSB, along with the Kvant Scientific Research Institute which assisted the FSB in technological research, was the primary agency engaged in developing Russia's offensive cyber capabilities. The FSB is believed to have coordinated the cyber-attacks conducted against Estonia and Georgia, with the GRU taking a backseat. At that juncture, the strategy of FSB sponsoring cyber-attacks to be carried out by non-state actors, wherein attributability could be denied, served Russia's interests.

(b) **GRU**. The cyber successes of Russia in Estonia and Georgia, however, prompted the US to shore up its efforts to militarize its cyber capabilities, notably with the formation of its Cyber Command in 2009. This in turn triggered the GRU, in 2013, to set-up new military science units for carrying out R&D with focus on cyber operations. Also, the conflict in Georgia exposed serious operational and organizational deficiencies, including in the area of information operations, for the Russian armed forces. As a follow up, in 2014 Russia's Ministry of Defence announced the establishment of an "information operations force", and the 2014 Military Doctrine listed the

"development of forces and means of information confrontation" as a main task for modernizing Russia's armed forces. By 2017, it is estimated that the GRU was able to recruit considerable talent and became a leader in offensive cyber operations. An overview of the GRU resources which possess SCEIIO capabilities is as under:-

(i) Information available in the open domain indicates that the GRU organized its psychological operations specialists into eight "operational groups" at around the time of the first Chenchen War in the mid-1990s, and the nucleus of GRU's psychological warfare apparatus in the 72nd Special Service Center (Unit 54777).

(ii) Further, the 85th Main Special Service Center (Unit 26165), which was responsible for GRU's cryptography during the Cold War, has perhaps now been re-focused towards offensive cyber operations.

(iii) Another unit tasked for offensive cyber operations is the Main Center for Special Technologies (Unit 74455), which was presumably involved in the effort to influence the US presidential election in 2016, the NotPetya attack of 2017, as well as cyber operations in Ukraine, amongst others.

(iv) As is evidenced by many reports, Russia continues to invest in and develop its CIO capabilities, using a combination of SCEITO and SCEIIO to achieve strategic cognitive effects in and through cyberspace.

(c) **Non-State Actors**. Some of the more prominent non-state actors being exploited by Russia for CIO are as under:-

(i) The Internet Research Agency (IRA), also referred to as TEKA, a Russian company owned by the oligarch Yevgeny Prigozhin who is known to be closely associated with the Kremlin, is the primary non-state agency being used by Russia to push its agenda. It is estimated to have about 1000 operatives tasked with daily targets allocated in terms of the number of comments, shares, likes, etc on social media platforms.

(ii) APT 28 (also known as "Fancy Bears", "Pawn Storm", etc), is generally understood to be a non-state actor. However, as per claims of cyber-security companies such as FireEye, SecureWorks and Microsoft, it may actually be an FSB/ SVR/ GRU unit(s). The main targets of APT28 are the Caucasian (primarily Georgian) and Eastern European countries.

(iii) APT29 (also known as "Dukes") is another non-state actor linked to the Russian hierarchy, which is known to be working with the Russian Federation since 2008.

China

22. Beijing, too, has long viewed control over ideas as a core tenet of China's national power. The Chinese Communist Party has increasingly sought to apply these concepts of control beyond its borders, and its efforts to shape the global online information environment have gained prominence in the CCP's foreign policy agenda in the last decade. Dating back to the late 2000s at the height of Hu Jintao's leadership, the CCP's Central Propaganda Department (CPD) sharpened its focus on

the global "competition for news and public opinion" and "the contest over discourse power" through the "innovation of news propaganda." Shortly after becoming the general secretary of the CCP, Xi Jinping reiterated at the August 2013 National Meeting on Propaganda and Ideology that China needed to "strengthen media coverage … use innovative outreach methods … tell a good Chinese story, and promote China's views internationally." A 2013 meeting of the CPD reiterated that shaping online public opinion was an area of "highest priority" for the party. Through propaganda, censorship, and strategically motivated economic coercion, Beijing has sought to tighten its chokehold on self-proclaimed "core interests" such as Taiwan; forestall international criticism of its policies toward Hong Kong, Tibet, and Xinjiang; and promulgate narratives about its global leadership.

23. A wide range of state actors have a hand in these efforts, including the Ministry of Foreign Affairs, State Council Information Office, the Central Foreign Affairs Office, the United Front Work Department, the Ministry of State Security, the Ministry of Public Security, and the Cyberspace Administration of China, to name a few. Additionally, on the military side, the reorganization of the People's Liberation Army (PLA) in 2015 and the consolidation of its cyber capabilities into a single service PLASSF generated significant momentum for Beijing's concept of "information warfare," including through the development and deployment of new platforms. (Daniel Kliman, et al 2020).

24. The Chinese version of Information Operations is captured in their concepts of *Integrated Network Electronic Warfare (INEW)* and *Three Warfares* . The INEW concept is based on the convergence between CO and EW, which is now chartered to

the PLA Strategic Support Force (PLASSF). The Three Warfares theory covers Psychological Warfare, Media Warfare and Legal Warfare, and its conduct is the operational responsibility shared by the SSF as well as the Political Work Department (erstwhile General Political Department), which functions directly under the Central Military Commission (CMC). This theory reflects China's intent to make a strategic shift from engaging in kinetic conflicts to waging political warfare.China is believed to have evolved its version of IO after an in-depth study of US concepts and literature. However, while US doctrine largely restricts information domain activities to military operations, the Chinese perspective is more aggressive, viewing IO as continuous across the spectrum of conflict, thus blurring the boundaries between peace and war.

25. **Integrated Network Electronic Warfare (INEW)**. INEW is one of the two concepts which drives Chinese doctrinal thought on IO. In a seminal article by Dai Quingmin, a leading IO proponent in the PLA, INEW is the "organic combination of electronic warfare and computer network warfare" . Enunciated in 2002, this concept was considered revolutionary, as it recognised the importance of achieving convergence between the seemingly diverse fields of CO and EW. The INEW concept finds a parallel in the US Army notion of *Cyber Electromagnetic Activities (CEMA)*, which however has not yet been adopted at the DOD level.In generic terminology, INEW and CEMA may be termed as Information-Technical Operations (ITO), a logical grouping of IO disciplines distinctly different from Information-Psychological (or Cognitive) Operations (IPO) or Inform and Influence Operations (IIO). In relation to CIO, SCEITO would find its moorings in INEW/ ITO.

26. **Three Warfares**. In 2003 the CCP Central Committee and the CMC adopted the concept of the Three Warfares in the revised "Chinese People's Liberation Army Political Work Regulations". Out of its three components, Psychological Warfare and Media Warfare resonate with various conceptualisations of Cognitive Operations, while Legal Warfare is a unique Chinese concept. The SCEITO sub-stream of CIO is a manifestation of the Three Warfares concept in cyberspace. Briefly, the three components may be defined as under :-

(a) **Psychological Warfare** seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations.

(b) **Media Warfare** is aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests.

(c) **Legal Warfare** uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be used to thwart an opponent's operational freedom and shape the operational space. It is also used to build international support and manage possible political repercussions of China's military actions.

27. **CIO : Overall Strategy**. Unlike Russia which is widely believed to have conducted aggressive CIO in conflict scenarios such as Estonia, Georgia and Ukraine,

there is no evidence of similar campaigns having been conducted by China, with its intrusive activities in cyberspace largely confined to cyber espionage. This is perhaps because the strategic objectives of China are quite different from those of Russia, as under:-

(a) At this juncture, the primary objective of CCP propaganda is to project China as a peace-loving country, with a trustworthy leadership, and present itself as a global player. The "Chinese Dream" is portrayed as being beneficial to the international community as well. At the same time, it also seeks to undermine values such as freedom of speech and religion which are seen to be threatening to its authoritarian culture.

(b) China has promoted a model of *cyber sovereignty*, which propounds the right of the state to exercise control over national cyberspace. President's Xi's well-known remark that "without cyber sovereignty, there is no state sovereignty", summarizes this concept.

(c) Towards this end, influence operations are aimed at both domestic and international audiences, and specifically target cultural institutions, media organisations as well as business, academic and policy communities.

(d) Although a significant part of Chinese influence operations is conducted by non-cyber mechanisms such as broadcast media, Confucius Institutes, etc. CIO play a major role in the overall strategy. The media houses

in China being almost entirely state-owned or controlled, online platforms of media organisations such as Xinhua, CGTN and the People's Daily are focused towards influencing foreign audiences. These organisations are also very active content generators on western social media platforms.

28. **CIO : Specific Examples**. A more belligerent flavour of Chinese influence operations in cyberspace has been observed against the backdrop of its recent aggressive and expansionist moves in Ladakh, Taiwan, South China Sea and Hong Kong. Some examples of specific influence operations in cyberspace carried out by China are as under:-

(a) In 2017, the German government levelled the charge that Beijing had used LinkedIn and other social media to target more than 10,000 of its citizens to influence and possibly recruit them for intelligence operations, including lawmakers and other government employees.

(b) There have been reports that China is carrying out psychographic profiling of political, military and scientific top brass in India in preparation for follow-up CEIIO at the appropriate time (Christopher Balding & Robert Potter, 2020).

(c) Unlike Russia, there was not much evidence of China interfering in the 2016 US presidential elections, and only feeble attempts were made to influence the 2018 US mid-term elections. However, China was more actively involved in the recent 2020 presidential elections, although the intent was

apparently to create confusion and chaos amongst the American electorate. There were reports that the Chinese were supporting Biden and Trump's ouster.

(d) However, the Chinese have been actively involved in elections in Taiwan, protests in Hongkong and COVID 19 related disinformation.

29. **<u>Military Organisations : PLA</u>**. Influence operations in China are coordinated at a high level and executed by multiple agencies including the United Front Work Department, the Propaganda Ministry, the Ministry of State Security and the PLA. In a major restructuring as part of ongoing military reforms, the PLA Strategic Support Force (PLASSF) was raised in Dec 2015,

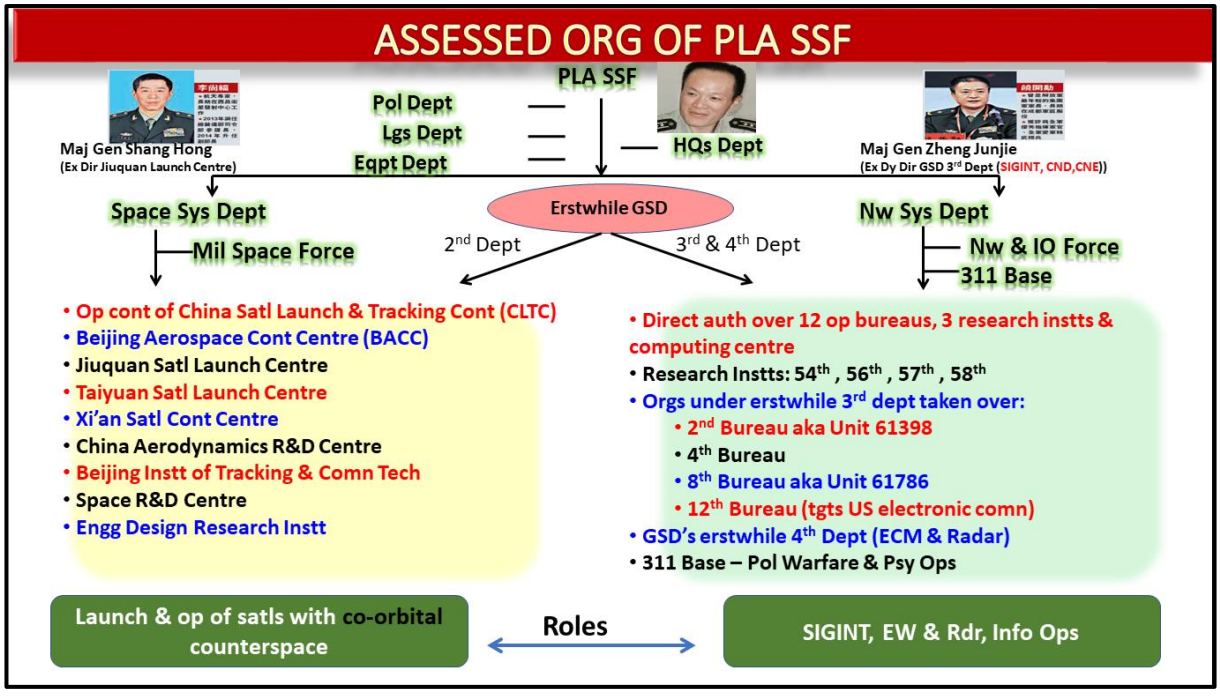


Figure 4.3 – Assessed Organization of PLA SSF

bringing most space, cyber, EW and psychological warfare capabilities at the strategic level under one jurisdiction **(Figure 4.2)**. The PLASSF comprises of two operational departments, namely, the Space Systems Department (SSD) and the Network Systems Department (NSD). The former controls nearly every aspect of PLA space operations, including space launch and support; telemetry, tracking, and control; information support; and space warfare. The NSD is responsible for cyber, electronic and psychological warfare**. Such a re-organisation also implies that *cyberspace and cognitive domains, together with electromagnetic domain, are being treated as warfighting domains in their own right,* rather than supporting elements in the traditional land, sea and air domains.** The integration of space, cyber, EW and psychological warfare capabilities under one umbrella may be contrasted favourably with the corresponding organizations in the US, where these capabilities are chartered to four separate unified combatant commands, namely, the US Space Command (USSPACECOM), the USCYBERCOM, the US Strategic Command (USSTRATCOM) and the USSOCOM. The creation of the SSF reflects the evolution of Chinese military thought, which now clearly considers information to be a strategic resource in warfare. The organisations and capabilities available with the CMC and the PLA for carrying out CIO, by leveraging CO and cognitive operations capabilities, are briefly discussed below:-

(a) **<u>Cyber Operations/ SCEITO</u>**. The NSD is responsible for PLA's cyber exploit/ espionage missions as also for cyber-attack missions. Such an integration reflects the felt operational need for close coordination between these two missions, as well as the commonality of expertise required for carrying them out. It is likely that the 12 Technical Reconnaissance Bureaus

(TRBs), which are mandated to carry out cyber exploit/ espionage as well as signal intelligence (SIGINT) missions, have been placed under the NSD. It is also expected that elements integral to the erstwhile GSD's Fourth Department, which were trained for carrying out cyber-attack missions, have also been transferred to the NSD, perhaps by integrating these into the TRBs. In addition, the 56th, 57th and 58th Research Institutes (RIs), which are known to possess the R&D and weaponization expertise for cyber as well as SIGINT missions, have also been placed under the NSD. Lastly, the PLA Information Engineering University has been moved to the NSD for enabling the necessary cadre development. It is to be noted that cyber responsibilities are also shared by the Network-Electronics Bureau (NEB), which is part of the Joint Staff Department (JSD) of the Central Military Commission (CMC). In addition, there are cyber elements placed under the theatre commands as well. Finally, cyber defence of networks is not entirely with the PLASSF, with responsibility for this being shared with the Information and Communication Bureau, which too is part of the JSD (JSD-ICB) [16]. The exact division of responsibilities between the JSD and SSF to fulfil cyber missions is not yet very clear.

(b) **Three Warfares/ SCEIIO**. In the pre-reform era, responsibility for the conduct of Three Warfares, also termed broadly as political warfare, was entrusted to the GPD. Within the GPD, political warfare at the strategic level was handled by the GPD's Liaison Department, while at the operational level this was carried out by the 311 Base along with its six subordinate regiments, all of which were placed under the command of the GPD. After the re-structuring, the GPD has taken the form of the new CMC Political Work

Department, while the 311 Base has been shifted to the SSF. Within the SSF, although the location of the 311 Base has not yet been confirmed, it is expected to be either under the SSF Political Work Department or, more likely, under the NSD. Since the PLA is inherently a party army and not a national one, one of its imperatives is to ensure ideological loyalty amongst its cadre and propagate party ideals. This aspect will now fall within the purview of the new CMC-PWD, while the operational effects of Three Warfares across the entire spectrum of conflict would be the responsibility of the SSF, thus achieving a decoupling between party and military requirements. Finally, while some aspects of psychological warfare have evidently been shifted to the SSF, the other two components of "Three Warfares", i.e. legal warfare and public opinion warfare, fall outside the SSF's charter.

30. **China's Propaganda Ecosystem : Organizational Structure**. Two pillars of the CCP's distinctive approach to controlling information are the Central Propaganda Department (CPD) and the United Front. Both encompass an alphabet soup of offices with shifting portfolios and positions in the parallel bureaucracies of party and state, but all ultimately report to policy making and coordination bodies ("leading small groups") at the apex of the CCP's leadership. Though they generally operate in extreme secrecy, their basic remit is to engineer domestic and international climates favourable to the Party's goals. As CCP General Secretary Xi Jinping tightens his grip on China and positions it for global leadership, their work has taken on new urgency (Renée Diresta, et al 2020).

(a) **Central Propaganda Department**. The CPD, China's first pillar of information control, lies at the heart of the CCP's propaganda apparatus. Established in 1924, it was patterned after the Agitation and Propaganda Department of the Central Committee of the Communist Party of the Soviet Union. In time the CPD's tendrils penetrated every channel of mass communications in China, policing content from print publishing and broadcast media to cyberspace, the arts, and education. The CPD also presides over the ideological indoctrination of party members and supports the propaganda ("publicity" is now the CCP's favoured translation) activities undertaken by ordinary government offices. Formally, it coordinates with state organs in charge of areas such as law enforcement, media licensing, and internet regulation, but in practice the boundaries between these bodies blur. Some of them represent themselves domestically as party organs and externally as state organs, and many of the relevant personnel have dual party and state identities. For instance, the State Council Information Office is the externally facing, state alter ego of the Foreign Propaganda Office of the CCP Central Committee. In June 2020, it released a government white paper that extolled China's response to the COVID-19 pandemic.

(b) **The United Front**. The United Front, the second pillar, maintains a comparable dual identity. Managed by the CCP's United Front Work Department (UFWD), it co-opts influential figures and groups that the CCP finds useful but does not trust, such as non-party intellectuals, academics, and business people. It operates through a web of overt and clandestine activities and organizations both within and outside of China, including cultural

exchanges, religious groups, professional societies, criminal gangs, chambers of commerce, peaceful unification committees, and many other ostensibly civic associations. Along with the People's Liberation Army and the Party, Mao listed the United Front among the three "magic weapons" that achieved the revolutionary victory that first brought him to power. During the Korean War, it managed the foreign exponents who helped to give China's germ warfare allegations global reach. Today, it orchestrates localized influence campaigns around the world.

31. **China's Overt Influence Capabilities : Controlling Information Domestically**.

(a) In the late 1990s and early 2000s, with the advent of economic reforms and the internet, media in China enjoyed a golden era of sorts. Crusading newspapers and magazines ran investigative pieces, such as exposés on an HIV epidemic in rural China and reports on police torture that probed the darker corners of Chinese society. The rise of social media—such as Weibo and WeChat—further challenged the Party's monopoly on speech by surfacing new voices. Beginning in the mid-2000s, however, the Party conspicuously began to reassert control. It replaced editors and publishers at many of the more popular media outlets, and the CPD banned Chinese media in one province from conducting investigative journalism in another. As an example of the increasing harmonization of the media around Party messaging, major national newspapers have on several occasions printed nearly identical front pages. At the same time, internet regulators have blocked a growing list of

foreign news, NGO, and social media websites, and have mandated real-name registration across a wide array of domestic online platforms, including Weibo. This has made it easier for the security services to interrogate, arrest, and prosecute Chinese netizens for expressing their political views (Renée Diresta, et al 2020).

(b) Regulators have also enlisted the firms that operate China's internet infrastructure in online surveillance by conditioning their business licenses on compliance with an unending stream of censorship directives. Finally, the Party has fostered a vast infrastructure of partisan commenters known as the 50 Cent Party to amplify its views and attack independent voices online. The 2011 Arab Spring rattled the CCP by demonstrating how threatening foreign social media and online platforms could be to the survival of authoritarian regimes. The following year, Xi Jinping came to power determined to stave off a "colour revolution" in China by "waging a war to win public opinion" and "retaking the Internet battlefield." The climate for free expression has since grown ever more repressive, and alternative points of view have been silenced across PRC society.

(c) In February 2016, Xi made a high-profile tour of the country's three top state-run media outlets, announcing that editors and reporters must pledge absolute loyalty to the Party and follow its leadership in "thought, politics and action." At the headquarters of China Central Television (CCTV), he announced that "the media run by the Party and the government are the propaganda fronts and must have the Party as their last name." In response,

state media redoubled what is euphemistically called "public opinion guidance": dissemination of content that touts the CCP's achievements, maligns its enemies, and makes its ascent appear inexorable.

(d) In 2018, the CCP further tightened party control of the media by shifting direct oversight of print publications, film, press, and a trio of key broadcast properties from state organs to the CPD. This trio, comprising China National Radio, China Radio International, and China Central Television (CCTV), including its international arm, China Global Television Network (CGTN), was merged into a media group known as the Voice of China, a move that broke down bureaucratic walls and facilitated unified messaging across the domestic and international media spaces in a multiplicity of languages. Fragmentary statistics suggest that, under Xi, the budgets allocated to propaganda organs at every level of government have swelled. This spending now supports the most sophisticated infrastructure of media surveillance and censorship on the planet.

32. **Projecting Influence Internationally**. While the CCP carefully polices its domestic walled garden, it exploits the freer spaces outside of China's borders to project its influence on the world stage (Renée Diresta, et al 2020).

(a) Since the mid-2000s, the Party has launched a campaign to grab "the right to speak" to the rest of the world from Western media outlets and independent Chinese-language voices, which it accuses of distorting news about China. For instance, in 2007, the Party unveiled a Grand External

Propaganda Campaign, earmarking billions in an attempt to control external narratives about China, and Xi has vastly intensified that effort, waging a global "discourse war". As Xi told the 2018 National Meeting on Ideology and Propaganda, "We should improve our international communication capability, tell China's stories well, disseminate China's voice, show an authentic and comprehensive China to the world, and raise the country's soft power and the influence of Chinese culture." To achieve those missions, PRC state media has greatly expanded its overseas operations. Xinhua, China's official state news agency, is one of the largest news agencies in the world. CGTN operates dozens of foreign bureaus and broadcasts in seven languages. China Radio International has contracts to broadcast from more than a dozen radio stations in the United States alone, while China Daily places inserts in newspapers such as the *Washington Post*, for as much as $250,000 an issue. PRC diplomats are actively promoting China's stories through regular, and sometimes pugnacious, appearances in local media around the world, a practice described as "Wolf Warrior diplomacy".

(b) PRC state media also successfully competes against established Western wire services to supply content to local media around the world. While generally uncontroversial, this content often repeats crude propaganda and disinformation on matters closely tied to PRC national interests. For instance, in March 2020, Press TV, an Iranian network aimed at the Middle East, reprinted a *Global Times* article that linked the origins of the COVID-19 pandemic to the U.S. military. Likewise, in May 2020, the *Manila Times* carried a *Global Times* article that argued that Taiwan bought passage of

supportive U.S. legislation through huge “donations” to American experts and scholars. State media has also expanded its foreign influence through social media channels, as detailed later in this paper.

(c) The global Chinese diaspora is a major, but often overlooked, audience for China’s propaganda. Thirty years ago, Chinese-language media outside of China reflected a diverse range of political perspectives. Today, after significant investment from China and pro-CCP interests, Chinese language publications that echo and amplify CCP narratives dominate. Chinese state actors are believed to have directly established some of these outlets, such as the U.S.-based media group that owns the television station SinoVision and the newspaper *Qiao Bao*. This media group was founded by reporters and editors from China who immigrated to the United States in the 1990s. Originally set up after the 1989 crackdown on pro-democracy protests in Tiananmen Square to burnish China’s standing in the Chinese diaspora, it maintains close ties with state-owned media and entertainment organizations on the mainland.

(d) In parallel with the state media’s international inroads, the United Front has been vital to China’s soft power offensive. Broadly speaking, all party members are obliged to promote the United Front’s mission, but those serving in commercial, cultural, educational, and professional organizations, along with other forms of “people-to-people” exchange, are at its forefront. The United Front cultivates pro-Beijing perspectives in the Chinese diaspora and the wider world by rewarding those it deems friendly with accolades and

lucrative opportunities, while orchestrating social and economic pressure against critics. This pressure is often intense but indirect, and clear attribution is therefore difficult. But it has had a devastating effect on Chinese-language media in the diaspora.

(e) Only a handful of independent voices remain in North America, Australia, and Europe, though Southeast Asia's landscape is more diverse. Meanwhile, China's government has brought hundreds of journalists from developing countries to China for training courses that showcase the economic and technological achievements of China's governance model. The Chinese government typically pays their expenses, offers stipends, and provides generous accommodations and sightseeing opportunities, which return dividends in goodwill and favourable coverage when the journalists return home. Xi Jinping has energized the UFWD's operations, reportedly adding 40,000 officials to its roster and elevating it to the top tier of party organs. Able to tap the party-state's vast resources, it realigns interests and incentivizes cooperation with the CCP so that influential non-party figures naturally take up and amplify the Party's talking points as if these were their own. Ideally, foreign partners have no idea that they are targets of United Front operations, making the enterprise particularly effective. One such case is that of Sweden's former ambassador to China, Anna Lindstedt, who abetted an effort by apparent CCP surrogates to silence one of the most forceful international critics of the Party. Had it succeeded, this old-fashioned human operation would have eliminated a vital challenge to the dominance of the CCP's modern propaganda machine.

33. **Making Overt Propaganda Social**. In addition to China's influence methods in the traditional media ecosystem and on domestic digital platforms such as Weibo, Chinese state media has expanded its international influence by establishing a social media presence (Renée Diresta, et al 2020).

(a) Starting at least as early as 2009, the properties have leveraged a broad range of Western social media platforms, many of which are blocked in China itself (**Figure 4.3).** On Facebook alone, Pages belonging to China's English-language state media apparatus give the CCP access to, at a minimum, over 100 million followers on the platform worldwide. Since 2015, the CCP has pursued a strategy of media localization on social media, including the use of regionalized language and content. This is particularly evident on Facebook: CGTN, for example, maintains CGTN America, CGTN Europe, CGTN Africa, CGTN Français, CGTN Arabic, CGTN en Español, and CGTN на русском (CGTN in Russian) as official Pages on the platform. Much of the content appears to promote a positive view of China and its place in global politics and culture. For example, English-language Chinese state media coverage has consistently taken a positive tone in its coverage of the coronavirus pandemic, sharing a significantly higher percentage of positive narratives —such as stories of recovered coronavirus patients—than U.S. mainstream and government-funded media on this topic.

(b) Chinese state media uses paid ads to push content from these Pages into the social media feeds of people across the globe. **Facebook's Ads Library shows regional ad targeting of the English language content to a**

wide range of countries including India (Punjab State), Nepal, Bangladesh (Dhaka), and the Philippines (Manila), suggesting that English is used to communicate state views to a broad global audience. Chinese state media outlets are not the only official Chinese channels spreading Beijing's narrative on social media: several Chinese diplomats and embassies have created active presences on Twitter since early 2019.50 Some of these accounts have hundreds of thousands of followers, such as Foreign Ministry of Information Department Director Hua Chunying, with 575,300 as of July 2020;Zhao Lijian, a spokesperson at the Ministry of Foreign Affairs renowned for his combative commentary on the United States, has more than three quarters of a million followers. Numerous Chinese editors and reporters are also active on Twitter. For instance, Hu Xijin, the editor of *Global Times*, has 404,100 followers and tweets regularly.

Figure 4.4 – Chinese State Media Accounts on Social Media

	Official Presence On Platform			
Outlet	**Twitter**	**Facebook***	**Instagram**	**YouTube**
Xinhua News	12.6M	79.9M	1.2M	894K**
CCTV	1M	49M	779K	857K**
CGTN	13.9M	105M	2.1M	1.66M**
People's Daily	7.1M	84M	1M	64.3K
Global Times	1.7M	54M	174K**	34.5K**
China Daily	4.3M	93M	603K	27.9K**
China.org.cn	1.1M	32M	N/A	11K**

Table 1: *Number of followers of official Chinese state media accounts on social media as of May 29, 2020.*
** Facebook number represents how many people have Liked the Page.*
*** indicates the account has not been verified by the platform.*

34. **China's Covert Influence Capabilities**. China's extensive overt propaganda capabilities, on print, broadcast, and social media, are used to influence audiences both domestically and worldwide to embrace China's point of view and policy positions. Although those messages may involve persuasion, spin, and factually dubious claims at times, they can be directly tied to their state-actor source. However, as with many states, China additionally has less-attributable or unattributable communication options that it can draw on to influence opinions more surreptitiously. These include content farms, subversive commenter brigades, fake social media accounts and personas, and misleading actors on social media channels (Renée Diresta, et al 2020).

(a) **Content Farms**. One facet of China's present-day means of influence is content farms (sometimes called content mills): websites that mass-produce clickbait articles designed to generate traffic and ad revenue.

(i) They may be multinational operations made up of many individuals who earn substantial amounts of money by either creating or sharing the articles, often plagiarizing content from other sources. To facilitate distribution, some drive traffic to their site through search engine optimization (SEO) techniques; others share content to social networks or post their links on popular messaging platforms. The opaque nature of the funding, ownership, distribution, and relationship to the state makes content farms a modern digital variant of the grey propaganda media properties of decades past. Content farms are a global phenomenon, but those with content related to the PRC are most

often based in China, Malaysia, and Taiwan. Audiences vary: some generate content aimed at the Chinese diaspora living outside the mainland, while others target audiences of strategic interest, such as those in Taiwan. According to an April 2020 report from Recorded Future's Insikt Group, there have not yet been observed cases of state-linked English-language content farms targeting Western audiences.

(ii) The Reporter, a Taiwanese non-profit media organization, undertook an extensive investigation into the dynamics of the farms, tracing them from their posts on LINE, a Japanese mobile messaging app popular in Taiwan, back to their owners. Some of the owners have personal pro-China political leanings, which is reflected in the content on their sites. In an interview with The Reporter, Evan Lee, a businessman who runs multiple content farms, described the websites as having two potential motivations. Farms with financial motivations generally produce "trivial articles" that focus on topics from health to fashion to history. Others, Lee says, have "an agenda," and are motivated by political or social interests rather than money; some of these farms occasionally feature disinformation and conspiracy content. Content farms with a covert political agenda promote pro-China stories while also amplifying or initiating denigrating rumours about political opponents, such as Taiwan's government under President Tsai Ing-wen. Some of the political content farm material appears to be plagiarized from Chinese outlets: Taiwanese fact-checking website MyGoPen has reported finding simplified characters, phrases used only

in China, or official statements from the Chinese government in the suspicious articles users saw online and flagged for fact-checks.

(iv) The Insikt Group's report also finds that this amplification relationship has worked in the opposite direction. In 2018 a false story about banana exports was framed as an example of the DPP's responsibility for Taiwan's deteriorating relationship with China; it was created by the content farm "Mission," which, according to its WhoIs records, is registered in Taiwan. It was picked up by China-friendly media outlets in Taiwan, such as *China Times* and *United Daily News*, and then by Beijing's state-run press agency, Xinhua News Agency. The spread of stories from grey propaganda content farms to more legitimate press with a wider audience, including state media, is a modern form of narrative laundering. Although journalists and researchers who study China have noted the presence of these grey propaganda properties and their frequently sympathetic stories about China, attribution of *specific* content farms as direct tools of the Chinese government remains a challenge; for example, The Reporter describes the domain read01.com, as a Chinese content farm. This content farm was highlighted in their investigation because it amplified a rumour in one of its articles. Read01.com's articles are written with traditional Chinese characters, which are used in Taiwan but not in China. However, according to its WhoIs record, the domain was previously registered in China, then switched to an American-based Cloudflare IP in 2016—which some operators do to mask their identity

and country of origin. Nonetheless, domain registration alone is insufficient to assert that a given content farm is part of a state-sponsored influence operation.

(b) **Surreptitious Commenters : The 50 Cent Party**. Perhaps the most famous of China's more covert influence capabilities is the digital commenter brigade known as Wumao, or "50 Cent Party." It emerged as a presence on China's domestically focused message boards and online spaces in 2004. The "army," as it is sometimes called, consists of hundreds of thousands—some estimates reach as high as two million—of conscripted posters who comment on social media and news articles to bolster the CCP, its leaders, and its policies, or simply to distract real participants from controversial topics and conversations. The scale of the operation is believed to be substantial, though exact estimates vary. In 2017, Gary King, Jennifer Pan, and Margaret Roberts undertook a comprehensive review of material from the 2014 "Xiaolan" leak of thousands of emails, in which 50 Cent Party posters submitted their online activity to the Zhanggong district Internet Propaganda to secure compensation for their completed assignments. The researchers posited that out of an estimated 80.4 billion social media posts in China's 1,200 or more online communities in 2013, 448 million comments were likely to be from the 50 Cent Party. On the surface, these posts appear to be the comments of ordinary people. King, Pan, and Roberts discovered that a majority of 50 Cent Party comments that included URL attribution appear to have been posted to government websites (GanzhouWeb, Newskj, DajiangWeb, JidanWeb, JiangxiWeb, CCTVWeb, RenminWeb, JiujiangWeb, and QiangGouWeb);

over 46% were on commercial sites including Sina Weibo, Tencent Weibo, Baidu Tieba, and Tencent QZone. The researchers found no evidence of automation in the posting process, but did note bursts of activity that indicated temporal coordination of comment campaigns. They additionally noted there was a minimal amount of what the researchers called "Taunting of Foreign Countries" in the 2014 dataset of leaked emails; most activity was focused on domestic topics, rather than international influence. Leaked documents additionally indicate that 50 Cent Party commenters are trained in an online "guerrilla ethnography" to help them understand their audiences. In a 2017 *Washington Post* op-ed, Blake Miller, of the London School of Economics, and Mary Gallagher, of the University of Michigan, describe the Chinese government's strategies to "guide public opinion as it develops": commenters are instructed, in official manuals, to drive and shape the conversation, "diluting negative attitudes online and spreading positive energy ." Gallagher and Miller reiterate that the strategy is not always unified within the domestic social media ecosystem; sometimes the censors who delete comments unacceptable to the Party work at cross-purposes to the paid army posting them. Although the execution appears to be haphazard at times, China's army of state-controlled internet commenters affords it the ability to introduce persuasive communications into the social media experience of Chinese "netizens," potentially creating the belief that engineered comments are the real opinions of fellow citizens just like them.

(c) **Covert Activity on Western Social Media Platforms**. Although attribution is often a significant challenge, the CCP has demonstrably begun to

expand its controlled-commenter-brigade strategies to Western social media. Some of the earliest indications of persona accounts on Western platforms appeared in March 2019, when BuzzFeed reported on allegations by Reddit moderators on a series of subreddits, noting the presence of what appeared to be coordinated efforts to downvote negative commentary on China in general and Chinese company Huawei in particular, and to upvote or push pro-CCP content. One moderator told BuzzFeed that "ironically, our freedom of press and an open internet is being exploited by an adversary to subvert democracy." BuzzFeed investigated thirty of the accounts, noting the difficulty of assessing the extent to which the efforts were coordinated; some of the accounts, in fact, acknowledged their connection to China by way of heritage or citizenship. Reddit ultimately did not make any formal attribution to CCP in its own investigation.

European Union

35. As a financial and political bloc of countries, the EU has responded to Disinformation against its member states primarily through defensive measures. These measures merit to be noted and should inform an Indian effort to configure organizational structures for SCEIIO. With concerns about social media disinformation campaigns multiplying and the European Parliament elections approaching, in 2018 the European Commission took several steps to tackle the risks of online disinformation. It,

(a) Convened a High-Level Expert Group to discuss how to address the issue.

(b) Created and financed a task force focused on countering Kremlin-led disinformation campaigns.

(c) Developed a secure online platform for Member States to share data and trends about disinformation campaigns.

(d) Fostered coordination of national electoral networks.

(e) Required internet platforms to develop and sign to a self-regulatory code to fight disinformation and used it to press the companies to do more and better ahead of the EP elections.

36. **Organizations / Initiatives : EU**. EU created bespoke organizations and initiatives to counter Disinformation as follows (James Pamment , (2020) :-

(a) **The EEAS Strategic Communications Division** There are two specific divisions within the European External Action Service (EEAS) tasked with assuming various strategic communications responsibilities relevant to disinformation. The Communications Policy and Public Diplomacy side leads outreach to EU and external audiences on EU foreign affairs, security and defence, and external action, developing political communications on behalf of the high representative for foreign affairs and security policy. It provides guidance, training, and strategic support to EU delegations and missions/operations. The division also manages communications campaigns,

internal communication, social media accounts, and digital platforms as well as public and cultural diplomacy. It does not have a formal role related to disinformation but rather fulfills advocacy and engagement functions for political and cultural EU objectives, including support to all digital media campaigns. The Task Forces and Information Analysis side focuses on the Western Balkans and Europe's eastern and southern neighbourhoods. Its main role is to develop and implement proactive communications activities and campaigns, including political advocacy and initiatives in public and cultural diplomacy for these regions. It provides analytical support for evidence-based communications and policies and has a specific mandate to address disinformation and foreign manipulative interference in the information space through the task forces (see below). It is responsible for implementation of the EU's Action Plan Against Disinformation and the Rapid Alert System (see below) and for the development of future policy in this field. It also has the mandate to support independent media and civil society in the two neighbourhoods and the Western Balkans.

(b) **The East StratCom Task Force** The EU first addressed disinformation as a matter of priority for security reasons. Following its annexation of Crimea in February 2014, Russia demonstrated disinformation to be a key method of hybrid warfare. In response to representations from a small group of concerned member states, the European Council "stressed the need to challenge Russia's ongoing disinformation campaigns" in March 2015. This push resulted in the creation of the East StratCom Task Force within the EEAS's Strategic Communications Division. The task force was established to

effectively communicate and promote EU policies toward the eastern neighbourhood; strengthen the overall media environment in the eastern neighbourhood and in member states, including by supporting media freedom and strengthening independent media; and improve the EU's capacity to forecast, address, and respond to disinformation activities by Russia. Many observers hoped that the East StratCom Task Force would find evidence of how Russian state-sponsored disinformation infiltrated Western media debates and support civil society to push back against it. The task force produces a weekly review of pro-Kremlin disinformation targeting the West as a flagship product on the EU vs Disinfo web platform, and its database features over 8,000 examples of disinformation. Its team has now grown to sixteen staff members with extensive (but presently outsourced) capabilities in the areas of media monitoring and strategic communications, following three years of funding from the European Parliament. This funding source expires at the end of 2020 and is not renewable.

(c) **The EU Code of Practice on Disinformation** The EU has also sought to collaborate with private companies to help stem the tide of hostile disinformation. In September and October 2018, it launched a Code of Practice on Disinformation together with roadmaps for implementation from partners in the private sector. Running for a twelve-month trial period (which covered the European Parliament elections in May 2019), the code was an experiment in voluntary self-regulation by the tech industry. Signatories made commitments in five areas: online advertisements, political advertising, integrity of services, transparency for consumers, and transparency for

researchers. Private sector partners published reports detailing their actions to mitigate disinformation. However, the signatories self reported their progress, and the information was not verified by an external body. The lessons from this process will feed into further EU policy developments in this area.

(d) **The Action Plan Against Disinformation** In December 2018, the European Commission launched its Action Plan Against Disinformation, which remains a key pillar of EU policy, granting mandates to several operational instruments. This measure placed disinformation within the context of hybrid threats and highlighted the role of strategic communications by the EEAS "as a priority field for further work." The action plan emphasized four areas of work: improving the capabilities of EU institutions to detect, analyze, and expose disinformation; strengthening coordinated and joint responses to disinformation; mobilizing the private sector to tackle disinformation; and raising awareness and improving societal resilience. It proposed maintaining the mandate of the East StratCom Task Force and reviewing the mandates of the Western Balkans and South Task Forces.The action plan recommended an expansion of their resources and capabilities, as well as the creation of a Rapid Alert System to strengthen coordination among EU institutions, member states, and other relevant international networks. It also proposed initiatives in the areas of strategic communications, media literacy, and high-quality journalism.

(e) **The Rapid Alert System** The EEAS launched the Rapid Alert System in March 2019 to enable common situational awareness related to disinformation spread across EU member states, as well as the development of

common responses. The system consists of a rudimentary platform for information sharing, as well as a network of points of contact in the various EU member states. The Rapid Alert System is intended to connect to existing real-time monitoring capabilities inside and outside of the EU, such as the Emergency Response Coordination Centre and the EEAS Situation Room, as well as the G7 Rapid Response Mechanism and the North Atlantic Treaty Organization (NATO), though this goal has been only partially realized. The system is therefore, in theory at least, an important platform for information sharing from an international perspective. So far, relatively few highly engaged EU member states share information through the Rapid Alert System. Major differences in how member states view the threat of disinformation are reflected in the use of the platform. In particular, a lack of trust between member states has led to low levels of information sharing and engagement. A successful aspect appears to be the networks and relationships formed among small coalitions of like-minded actors. Regular meetings have been held since early 2019, but the system's alert function had not yet been triggered as of June 2020.

(f) **Election Observation Missions**. EU-affiliated election observation missions also have a role to play. In October 2019, the European Council issued a document titled "Council Conclusions on Democracy," which observed new challenges to democracy emerging around the world. These include the undermining of democratic processes and institutions, low levels of trust, shrinking democratic space for civil society, increased violations of human rights and fundamental freedoms, and manipulation using online

technologies. This last point includes issues of disinformation, hate speech, privacy, and campaign funding. The European Council made commitments to strengthening the EU's democracy-building capabilities around the world, including promoting instruments created to mitigate the effects of online interference during elections. As a first step, election observation missions of the EU and its member states have been developing a methodology to monitor online political campaigns. In the case of EU missions, this methodology has been road tested in elections in Peru, Sri Lanka, and Tunisia, and it will become a standard part of all future missions. It will, in addition, create a basis for EU support to strengthen research, monitoring, and oversight capacities in third-country academic circles and civil society.

(g) **The European Democracy Action Plan and Digital Services Act**. In addition to the aforementioned measures, the European Commission is also developing two major new policies. First, it is preparing the 2020–2024 European Democracy Action Plan, which includes specific commitments to project EU values worldwide. This will likely include significant policy commitments at the intersection of disinformation, electoral protection, digital technologies, and public-private partnerships. In this regard, it will set out next steps for building on the Code of Practice and the Action Plan Against Disinformation. Second, building on existing e-commerce rules, the EU is preparing a Digital Services Act. Among other things, this measure will set out regulatory powers for the EU over digital platforms, which are likely to include powers of regulation and auditing relating to online disinformation.

37. The following list brings together the recommendations in a report outlining the framework for fighting disinformation against EU (Bruno Lupion, 2019):-

(a) **Build Stronger Analytical Capacity and Coordination Among EU Bodies** The EEAS StratCom team should be empowered to carry out deeper analyses to monitor disinformation campaigns. This capacity should be used also to inform the East StratCom Task Force, the Western Balkans Task Force and the Task Force South, to modulate their debunking and responses in their respective geographical areas. The EEAS StratCom team, in coordination with the three task forces, should continue to feed the Rapid Alert System with their monitoring and findings. The EU could have a senior officer or permanent structure to coordinate efforts to tackle disinformation.

(b) **Foster Coordination and Preparedness Among Member States** The fight against disinformation needs coordination among Member States. The Rapid Alert System should be strengthened. The EU institutions should support Member States to develop and improve their national monitoring systems of hybrid threats and disinformation, which in turn would strengthen the inputs received by the Rapid Alert System.

(c) **'Support Civil Society Organisations** Dealing with domestic disinformation or foreign disinformation spread by individuals or organisations based in the EU is difficult for the EU. The EU should leave this task to civil society organisations, which face less institutional constraints to investigate disinformation and have already demonstrated the capacity to do so. These organisations, however, face financial constraints and their analyses usually are restricted to a few countries. The EU should support initiatives and

make sure that monitoring continues between elections and covers all EU member states.

(d) **Address Co- or Normal Regulation** The EU should consider co- or normal regulation for some issues related to disinformation, such as political and issue ads, procedural standards for content regulation (e.g. appeal bodies), transparency on algorithm choices and ranking systems and the capacity the platforms put in place in each Member State. An opportunity in this regard is the new Digital Services Act, currently under discussion by the EC and expected to be revealed by the end of 2020.

(e) **Improve Media Literacy Among Citizens** The EC should support the inclusion of media literacy in school curricula and support similar projects for the elderly across-Europe. Likewise, it should support the inclusion of an assessment of students' media literacy competences in the next round of the OECD PISA test.

(f) **Political and Issue Ads** Companies should improve their APIs to allow researchers and journalists to smoothly query data from their ad libraries. Twitter and Google should also include issue ads in their transparency policies.

(g) **Improve Integrity** Although the companies have made efforts and built dedicated teams to increase integrity in their systems, this capacity should be greatly improved by combining AI and qualitative analysis. Civil society organisations with much less resources than the companies were able to spot malicious activity not identified by social media companies around the EP elections. YouTube should include rules to explicitly downgrade disinformation or forbid inauthentic coordinated behaviour in its policies, as

Google News policy do. Also, algorithms improvements, such as the Top News and Breaking News shelves, should be implemented across Europe.

(h) **More Coordination and Cooperation** Tech companies should deepen their coordination and cooperation efforts with governmental agencies, public bodies and civil society organisations. The experience has shown that multi-stakeholder approach is needed to tackle disinformation.

(i) **Revamping the Code of Practice** Internet platforms and the advertising industry should use the one-year assessment to discuss a revamp of the text and to satisfy requirements and current practices of self-regulation. They could use that opportunity also to pursue coordination on political and issue ads transparency policies, while the issue is not regulated at the EU level.

(j) **Fact-checking** Facebook should expand its partnerships with fact-checkers to analyse more content and reach all 28 EU countries. The initiative should also be permanently extended to Instagram to check disinformation spread via photos and memes. Twitter would benefit from a similar approach.

(k) **Empowering the Research Community** Facebook should invest more resources to solve technical 28 problems that are delaying the implementation of the partnership with researchers. Also, the company should unblock access via its API to public pages and posts.

(l) **More Coordination and Cooperation** Civil society organisations should press tech companies to increase coordination and transform findings into action. Also, it would be beneficial if CSOs manage to coordinate on which countries and which aspects of disinformation to monitor.

(m) **Adopting Common Reporting Standards** CSOs should discuss and adopt common reporting standards on methodologies and results.

(n) **Integrating Fact-checkers** Fact-checkers should partner with other organisations from civil society devoted to analysing social media dynamics. Insights brought by social media analysis would help fact-checkers act faster and before disinformation gets widespread traction. Also, European networks of fact-checkers should have an interface with official monitoring mechanisms and internet platforms.

CHAPTER V : RECOMMENDATIONS FOR NATIONAL ORGANIZATIONAL STRUCTURES IN INDIA

"The very conception of the information space as a domain of war is problematic for democracies."

- Laura Rosenberger and Lindsay Gorman

" When it comes to the external message, our narrative is being trumped by ISIS's. We are reactive – we think about 'counter- narratives', not 'our narrative' ".

-Richard Stengel

Concept of Victory in Information War

1. The US Information Agency, which coordinated the anti-communist communication plan, was a major player during the Cold War—pulling its weight in the yoke of overall Cold War strategy alongside the State Department's diplomacy, intelligence agencies' tireless clandestine work, and conventional military power and nuclear deterrence. The agency oversaw Radio Free Europe and Radio Liberty, and came to have 190 offices around the world, one of the broadest footprints of any Washington, DC–based outfit. They broadcast Voice of America in forty languages to reach more than one hundred million listeners, despite large-scale Soviet efforts to jam the signals; many people behind the Iron Curtain took great risks to tune in. The messages broadcast—of human rights, liberal democracy, and relative prosperity—proved irresistible. By the end of the 1980s, most of the Soviet satellite nations had broken free and, in the final week of 1991, the Soviet Union itself collapsed.

2. While it was just one pillar of a broader strategy, US-led messaging—both the message and the way it was delivered—was exceptionally potent. It was probably the strongest effort to bring down the Soviet bloc, rather than just contain it. The demise of the Soviet Union, in large part due to soft power and Western information campaigns, brings forth three vital lessons for the present day:-

(a) Firstly, just because authoritarian states are extensively employing it, that does not mean that information warfare is intrinsically anti-democratic and in an Indian way "Anti- Dharma". It can be entirely right for a nation (or any other entity) to project its messages beyond its borders. Information warfare was a strong pillar of the campaign against ISIS, for example, where it successfully stopped many vulnerable young men and women from traveling to Iraq and Syria to join the self-proclaimed caliphate. Information campaigns have been an important component of almost every modern war.

(b) Secondly, the demise of the Soviet Union suggests information wars have the potential to contribute substantially to the defeat of nations. And, if we are truly in an information age, then this danger has become more acute. Information warfare is not something trivial or secondary. It is a fundamental element of great power competition, and likely to play an ever-increasing role in future conflict.

(c) Lastly, it shows us that winning an information war is very different from defeating a single information campaign. A solitary piece of disinformation or propaganda can be neutralized: sometimes by locking it out of the media, occasionally by a fact-based rebuttal, usually by the concerted deployment of public relations techniques, and almost always by an equal and

opposite counter narrative. But winning the overarching information *war* is a very different concept.

3. The distinction between an information war and an information campaign is important. People are right to be alarmed at persistent efforts by authoritarian states to weaponize disinformation against democracies. But countering them, blocking them, and exposing them are only moves within information warfare. The defining feature of information warfare is that messages are the munition. Opponents in an information war usually have rival visions, as the United States and the Soviet Union did during the Cold War. It is a Clausewitzian clash of wills battled out through a broad conception of politics.

4. Winning a conventional war means extinguishing scope for organized violence to continue as before. **Hence, winning an information war means the previous direction of messages for a political or military effect is unalterably changed**. This definition fits neatly with the Cold War example: the information war against the Soviet Union was won when Moscow could no longer propagate credible pro-communist messages. To win the current information war—not just win a potentially endless series of battles—public debate needs to be safe from messages that seek to subvert the public interest. Of course, what the public interest is, and how malign messages are identified and excluded, are themselves hotly debated issues.

5. **Winning an information war is about putting certain ideas beyond contention, so that organized efforts to undermine them can have no traction.** Once that condition has been reached, democratic debate can concentrate once again on how to advance the public interest, safe from malign messages that seek to undermine that civic good. Battles over information will continue, however this has to

be fought strategically, not just tactically, for those victories in individual battles to mean the war is being won.(Iain King,2020)

Authoritarian Vs Democratic Systems

6. India's liberal democracy and highly diverse nature of the country is a very germane playground for Information/Influence Operations. Despite fairly strong and time-tested democratic structures, faultlines across class, caste, religion, language and geography are liable to be exploited by adversaries. With unsettled borders and proxy based secessionist movements having traversed the past few decades, Disinformation/Misinformation/Propaganda can be a potent tool for shaping operations during a conflict and Non-Contact Warfare across a seamless Peace/No War No Peace/War continuum. Proliferation of internet and social media proliferation provides a very potent medium for SCEIIO to be effected. Importantly, major adversaries that India faces viz, China and Pakistan are Authoritarian States with deep rooted cultures of centralized control and a propensity to employ Information as a weapon both within their countries and externally.

7. A major asymmetry between authoritarian and democratic systems is their view of information. Democracies believe in—and depend on—the open and free exchange of information that empowers citizens to make informed decisions to select their representatives and engage in political debate. They champion freedom of expression, association, and press as universal rights. The International Covenant on Civil and Political Rights captures this vision: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or

in print, in the form of art, or through any other media of his [sic] choice." Authoritarian regimes, by contrast, view information as a threat to state authority if allowed to flow freely and as an instrument of social control if managed and employed deftly. These regimes engage in censorship, surveillance, and propaganda, using the media and other tools to control and manipulate information on behalf of the state. Put simply, in democratic philosophy, information rests with citizens; in the autocratic vision, it rests with those in power (Laura Rosenberger and Lindsay Gorman, 2020).

8. These opposing visions of public discourse inform different approaches to an emerging twenty-first century struggle between authoritarianism and democracy that is increasingly playing out in the information arena. Authoritarian regimes like China see information and cyber warfare as integrated domains of asymmetric conflict distinct from kinetic operations. They weaponize information to fight back against democracies' promotion of free information as a universal right, which these authoritarian states see as a deliberate threat to regime survival. As Harvard university researchers Eric Rosenbach and Katherine Mansted have observed, authoritarian states offensively deploy information operations externally as tools of foreign policy, while defensively using propaganda and censorship as means of domestic control. In this autocratic approach, social media and online information platforms are weapons to be mastered to weaken democratic systems, alliances, and credibility. These regimes advocate internationally for a "sovereign" information space "where there are no universal norms, just zones of influence."

9. Though democracies have recognized the contest unfolding within and over the information environment, they have largely approached it in one of three ways: first, as a traditional question of public diplomacy and strategic communication, where the focus is on narrative content and the objective is to tell their story louder and better, hoping the truth will prevail; second, as an ancillary to kinetic warfare or other military operations, particularly the way technology and information abundance are changing the nature of kinetic warfare (even US thinking on cyberwarfare has traditionally focused on the use of cyberattacks to damage network infrastructure—not on the theft or manipulation of data itself for use as an information weapon); or third, as an economic or security challenge arising from technological competition, without considering implications for the broader information environment.

10. While these three approaches are necessary, each one focuses on a different aspect of the challenge in isolation—public diplomacy, the nexus to kinetic warfare, or technological competition—and none is sufficient. Instead, an effective strategy recognizes that the information arena has emerged as a domain of sustained and permanent competition that touches on all traditional aspects of national power. In other words, information is both a domain of operations in itself and an arena that affects all other traditional domains of nation state competition. Democracies' and autocracies' divergent views on information create asymmetries in the information domain—the very conception of the information space as a domain of war is problematic for democracies. Controlling and manipulating information is inherently more comfortable for and advantageous to authoritarian regimes, while it is inconsistent with democratic values and the function of democratic society. And construing information as a weapon or engaging in information warfare involving

non-military targets risks undermining the very space democracies seek to protect. As journalist and media scholar Peter Pomerantsev puts it, the authoritarian notion of "information warfare" is part of a world view and interpretation of history "where all values, ideals, ideas are mere fronts to subvert the other side, where there is no qualitative difference between independent journalism and a covert social media psy op."

11. The very notion of engaging in "information warfare" risks playing on a battlefield defined by democracies' authoritarian competitors and acceding to the closed, controlled, and manipulated view of information that authoritarians champion. But while democracies should not define this contest as "warfare," they need to recognize that their authoritarian adversaries do—and that such regimes believe democracies to be information aggressors, wielding information to undermine authoritarians' power and closed systems. Instead, democracies should understand the challenge as a global information contest that encompasses the use or manipulation of information (data and content) itself; the architecture, or the systems, platforms, or companies that transmit it; and the governance frameworks, including the laws, standards, and norms for content, data, and technology. This contest is a key avenue for advancing one system of values over another, and it both reflects and affects the broader geopolitical competition between authoritarians and democracies. Therefore, democracies must engage in a manner that affirms, rather than degrades, the information arena. The first dimension of this contest—the manipulation of information itself, primarily via digital means—At present, democracies are not meaningfully preparing for this struggle.

Strategic Imperative for Democracies : Address the Information Domain

12. While the information space as a contested domain poses challenges for democracies, they have little choice but to engage. Authoritarians are already contesting this domain and exploiting democracies' inaction. Whether or not democracies care for information warfare, information warfare is being waged against democracies. Democratic societies, where information flows openly, are particularly vulnerable to information manipulation, and authoritarian actors exploit this openness to weaken them. These regimes are filling the information space in areas of the globe where democracies' voices are absent. Contesting this space in a way that puts democratic values and principles about information at the centre is essential to preserving the democratic institutions that protect those values.

13. The use and manipulation of information to achieve national objectives is an increasing locus of great power competition. Although additional actors will adopt information manipulation tactics in this asymmetric and low-cost battle space, the primary information challenges to liberal democracies will continue to come from Authoritarian States like China due to their scope and sophistication. Operations short of armed conflict—many of which find fertile ground in the information domain—are becoming a mainstay of twenty-first century geopolitical competition. A national security paradigm that ignores information as a contested domain risks forfeiting some of the largest conflicts of the twenty-first century

14. While democracies need to contest the information space because of external threats from authoritarian competitors, they also need to combat the degradation of

their own information environments from within. Here, democracies face significant internal challenges. The emergence of what scholar Shoshana Zuboff calls "surveillance capitalism" as a business model incentivizes the surveillance of citizen data for profit and erodes privacy. The rise of information platforms with hidden inner workings for how content is prioritized and shown to users, like YouTube and Facebook's NewsFeed, provides a ripe target for algorithmic manipulation to advance divisive narratives and conceal external manipulation. And as some platforms have grown increasingly large, they have written the rules that govern wide swaths of the information space while remaining accountable only to their shareholders.

15. The failure of legal and regulatory regimes to keep pace with technology and ensure protections for a free and open information arena has perversely created room for authoritarian information models to expand and decreased the global attractiveness of open systems. Beyond the digital realm, the traditional media sector in many countries across the freedom and democracy spectrum has increasingly fractured, and the collapse of local and independent print media has created vacuums of quality information and undermined democratic accountability. Meanwhile, even private companies and media outlets in democracies are vulnerable to coercion by the Chinese Communist Party, which uses access to the valuable Chinese consumer market to compel favourable coverage and to suppress employee speech or corporate information on websites or products that counter the regime's strict censorship rules. Successfully competing in the information domain will require democracies to get their own houses in order (Laura Rosenberger and Lindsay Gorman, 2020).

Democratic Principles for Engaging in the Information Arena

16. How democracies approach this contest is therefore central to their success. Contesting the information arena should not mean jumping onto a playing field defined by democracies' adversaries. Rather, liberal democratic states must define their own terms of engagement that are consistent with the values they seek to protect. They must move from a reactive, tactical approach toward a proactive, sustainable, and strategic one. And they must recognize that their own shortcomings in protecting a healthy, open information environment have created space for competing authoritarian models. Ultimately, democracies' goal should be to promote a healthy, open, and transparent information arena as an element of the global commons. Such a conception stands in contrast to the authoritarian norm of cyber sovereignty, in which individual states set, control, and restrict their own information environments. The following principles should guide this democratic approach (Laura Rosenberger and Lindsay Gorman, 2020):-

(a) **Affirming The Value Of Information**. Recognize that while information can be and is being weaponized, information in and of itself is not a weapon. States that believe in universal values of human rights, freedom of information, and independent facts should avoid this reductive capitulation. Instead, democracies need to pursue strategies that affirm, rather than degrade, the value of information and its centrality to deliberative democracy. Quality of information is more valuable than quantity. Wikipedia is a prime example of a forum that—while not perfect—affirms the value of information and

prioritizes quality through a fair and open consensus-seeking process with trusted contributors and transparent mechanisms for adjudicating conflicts.

(b) **Openness**. Retain the open information systems that set democracies apart. That means setting an example by resisting the temptation to censor content. It also means fighting for universal—not sovereign—internet governance models and protecting open innovation and competition. Democracies will face hard choices in addressing threats from external actors, some of which may require imposing higher standards on the companies that participate in critical information sectors around infrastructure and personal data. But their bias should be toward remaining as open as possible.

(c) **Transparency** Establish transparency and accountability from both governments and technology. This principle applies to the handling of content such as political ads and the removal of illegal content by online information platforms. But it also applies to the structures that underpin and organize information, including the algorithms that select and deliver news, videos, and search queries. Transparency is an area where many democracies have fallen short and where redoubling focus will be essential to strengthening their hand.

(d) **Empowering Information Consumers**. Put users in control of their data and of how information is shown to them, allowing them to understand where their data is going and how it is shaping the content they are shown. Increasingly, algorithms invisibly shape our realities and guide our decisions. In the laissez-faire model, these algorithms are profit-driven. In the

authoritarian model, they are control-driven. Neither is good for democracy. In Peter Pomerantsev's vision, users should be "empowered to have a stake in the decision-making process through which the information all around us becomes shaped, with public input into the Internet companies who currently lord over how we perceive the world in darkness."

(e) **Truthfulness**. Employ factually verifiable information in democratic actors' own messaging, rather than simply blocking content from others. Importantly, while this normative principle should guide democratic actors' use of information, requirements of truth should not be legislated, imposed by democratic governments, or used as criteria for private actors moderating online content. For truthful ideas to succeed in an information-saturated world, they should look qualitatively different from falsehoods—by including trails for independent verification, even in today's information morass. A corporate statement or foreign ministry communique, for example, that included sourcing when making claims would build trust and credibility. The further politicians and public figures in democracies stretch the bounds of truthfulness, the more democratic societies lose the ability to distinguish fact from fiction. A world in which there is no objective truth is one in which democracies cannot succeed.

(f) **Civil Liberties**. Protect and respect civil liberties—core pillars of democratic societies—in the information commons. This principle includes protecting privacy from both state and corporate actors; preserving space for activist communities; safeguarding free expression and the freedoms of belief,

religion, and association that are increasingly under authoritarian attack; and upholding due process in an era of surveillance—both online and off.

(g) **Multilateralism**. The information contest is best understood as a competition between systems and values, not just of nations. Authoritarian information and influence efforts seize on divisions within and between democracies, while also targeting countries that feel unaligned. Eroding the international consensus around universal values is the autocratic mission. A multilateral approach with all of the aforementioned principles at its centre is the best defence against the authoritarian strategy of divide-and conquer.

What Democracies Should Do to Engage in the Information Contest

17. In the face of information manipulation from authoritarian actors, democracies should focus on two lines of effort for their engagement in the information arena: firstly, building information resilience in society and secondly, seizing the information initiative in accordance with the principles outlined above (Laura Rosenberger and Lindsay Gorman, 2020).

18. **Building Information Resilience: Fortifying the Democratic Model**

Authoritarian efforts to manipulate the information environment inside democracies leverage inherent asymmetries. But responding requires democracies to build resilience in their own information model while ensuring they do not create the hardened and closed information space authoritarian regimes promote. To do so, democracies must do the following:

(a) **Focus on Behaviour, Not Content, To Protect The Democratic Information Commons**. A reactive tendency to police content risks solidifying authoritarian norms of information control. For example, under the banner of countering "fake news," nations from Bangladesh to Brazil to Cambodia to France have put forth laws empowering governments to control information and in some cases punish the authors of what the government considers "fake news." Instead, to strengthen and affirm the value of information, the focus of defensive efforts needs to be on perpetrators and their modes as well as means of manipulation—not on suppressing content, which is itself a tactic of manipulation. Focusing on countering the underlying behaviour of actors engaged in malicious activity takes a more systemic approach to countering information manipulation than focusing on content, while upholding democracies' commitments to openness and freedom of expression. Whereas an authoritarian approach would censor speech by subject matter and, in some cases, imprison those responsible, democratic actors should look to expose and remove coordinated deception on the part of state and non-state actors.

(b) **Transparency From Online Information Platforms**. Engagement-driven metrics guiding the algorithms that organize, prioritize, and display information—and the opacity surrounding them—allow malign actors to degrade the information space by manipulating search results and promoting divisive content. Popular social media platforms that adhere to authoritarian censorship rules by removing or demoting certain content can also subtly

shape public perception, even in democracies. Reports of video-sharing app TikTok censoring content related to Hong Kong pro-democracy protests is a case in point. Without transparency requirements for the way information is displayed on information platforms, this manipulation is difficult to detect and assess. To build resilience against information manipulation, democracies should construct algorithmic transparency regimes to shine light on how information is prioritized online. While specific algorithms and computer code itself is proprietary information, companies could provide information on how algorithms operate without disclosing trade secrets or opening up their code entirely.

(c) **Data Protection And Privacy From The Private Sector And Empower Users Around Their Data**. In the information arena, authoritarian governments have seized on the collection of personal information on citizens as a means for manipulation and control. But democracies have struggled to protect citizen data from both authoritarian governments and corporations. Information manipulators collect personal data for a suite of uses: to more precisely target manipulation, to provide kompromat, to identify intelligence and counterintelligence targets, and to train artificial intelligence surveillance systems. Tech companies amass personal information and sometimes leave it unsecured, gift wrapping that data for malign actors. Here, a failure to empower users through robust and multilateral data protections renders democracies vulnerable to information manipulation and the dissolution of privacy as a universal right.

(d) **Build "Information Intelligence" Across The Public And Private Sectors**. Resilience against authoritarian information manipulation can only be as good as knowledge of it. But capabilities and prioritization here lag, and in a largely civilian domain on a private battlefield, there are inherent challenges for tracking these efforts in a manner consistent with democratic values. Specifically, democracies must balance an interest in monitoring for signs of information manipulation with the inherent collateral collection of information on their own citizens—even if that information is publicly available. A system that read, collated, and processed content from every Facebook account, for example, might be effective at detecting information manipulation on the platform, but in the hands of a government would pose serious problems for the privacy and civil liberties of its citizens. Online, this response should include careful information sharing among companies and government actors on inauthentic behaviour patterns and coordinated takedowns of this activity. Coordination across platforms has improved in recent years—such as when Twitter and Facebook together took down Chinese linked disinformation about pro-democracy protests in Hong Kong and disinformation from an Iranian network about the coronavirus in April 2020.But this balance should become muscle memory through a formalized approach. A principled response should also prioritize and support civil society and independent research efforts to study the information environment, particularly in the domestic sphere where democratic governments should not be conducting surveillance. In practice, building "information intelligence" requires coordination among the public sector, which can assess motives and nation-state strategy; the private sector, which houses information playing

fields; and civil society, with independent research capacity. As the information contest crosses borders, multilateral coordination on threat intelligence will be needed. But constructing this picture is not solely about social media monitoring. Democracies need to understand how their adversaries shape the broader information environment, beyond platforms. This holistic view stretches across society and includes the full complement of authoritarian information efforts: targeted media and diplomatic narratives, coercion of public and private sector actors, the manipulation of personal data for influence or control, the deployment of surveillance technologies, and international engagement to advance sovereign internet norms. Intelligence agencies will need to reprioritize open source information—where appropriate and consistent with their authorities limiting domestic collection—to recognize these broader tactics and integrate them into their understanding of adversary objectives. They will also need to inform broader segments of governments and societies on their findings. Six months in advance of Canada's fall 2019 elections, for example, its intelligence community's Communications Security Establishment released a public report on cyber threats to the nation's democratic processes, including the manipulation of information to influence voter opinions in the context of global trends. The report found that political parties, candidates, and staff; Canada's elections infrastructure; and Canadian voters themselves were all targets of malicious cyber activity and that the Canadian public was likely to see voter influence attempts through the manipulation of information online in the lead-up to the election. For a whole-of-society picture, governments, too, need to be transparent about the threats they face.

19. **Seizing the Information Initiative : Advancing the Democratic Space**

Democracies should embrace an external focus that communicates the attractive power of the democratic information model to democracies, autocratic populations, and in-between states while recognizing the internal work necessary to build a model that can compete with what authoritarians are selling. Ultimately, democracies should harness open and truthful information to proactively contest the information space and promote and defend a global information commons**. A possible framework is that of persistent engagement, which US Cyber Command has adopted to describe its continuous and proactive engagement to maintain initiative in cyberspace, to the information arena—not as a military doctrine, but as a civilian-led interagency effort.** This framework would recognize that the information contest is ongoing, falls outside as well as within the traditional boundaries of conflict, and must contend with adversaries' actions that are unlikely to be deterred. It also recognizes that in the information arena, democratic engagement must be ongoing due to a distinct first-mover advantage: setting the narrative is far easier than changing it, and information vacuums are readily filled. In the technical digital realm, unique, new, or uncommon search terms associated with breaking news or obscure queries create "data voids" where little authoritative content exists and manipulators can flood the zone with their content. In the geopolitical realm, unfolding events absent quality information and analysis create space for authoritarians to shape the narrative. To seize the information initiative and advance and harness the affirmative value of information, democracies should take the following actions:-

(a) **Align Policy With Credible And Truthful Messaging**. Since the end of the Cold War, democracies have neglected the importance of the information component of their actions, relying instead on the openness of the media to tell their stories. In the information age, effective policy needs an effective message. Too often, an absence of coordinated messaging alongside policy creates a vacuum that democracies' competitors fill. In 2014, Russia paired its invasion of Crimea with a significant information campaign advancing the narrative that Crimea was actually part of Russia, not Ukraine. Democracies failed, in this case, to provide an equally rapid and sophisticated response in the information domain. An integrated information component in policymaking includes analyzing the information effect of policy options as part of decisions, prioritizing an information strategy in policy implementation, identifying the best channels for disseminating and propagating information, and understanding likely adversary counter-messaging. In short, **integration of an affirmative information component into all government actions will be critical for contesting the information space and for ensuring the success of policies across all domains. This holistic integration also includes understanding that government is not necessarily always the right messenger and that marshalling trusted outside voices is often the best approach**. In addition to governments, private sector actors also need to develop strategies around information. Private sector entities need to develop affirmative approaches to messaging that ensure they—and not authoritarian regimes —set the terms, maintain the initiative, and protect the free flow of information.

(b) **Harness And Assert The Positive Value Of Open Information**. Finally, democracies should harness open and truthful information to contest the information space proactively. In practice, this harnessing involves joining with likeminded nations to point out failures of authoritarian regimes, spotlight censorship and condemn repressive acts in the information environment loudly, clearly, truthfully, and multilaterally instead of tacitly accepting them. Here, democracies can look to their militaries for inspiration: the US Navy conducts "freedom of navigation operations," patrolling open waters to protect open passage through internationally recognized waterways and challenge excessive maritime territorial claims. In the information domain, analogous "freedom of information operations" could protect an open information commons. On third-country playing fields, these operations could be deploying truthful messaging to spaces that authoritarians are attempting to fill and using information to pierce the narrative they seek to construct about themselves, such as in the case of the CCP's "discourse power" strategy that seeks to elevate CCP narratives and neutralize criticism abroad through engagement, agenda-setting, and propaganda. Funding independent journalism and publishing these outlets' standards of independence to showcase the distinction from authoritarian-funded and controlled media such as China's Global Times could also be part of this picture. In autocracies, "freedom of information operations" could be technological efforts to mute the effectiveness of authoritarian information control mechanisms like China's Great Firewall that blocks access to foreign websites deemed problematic or Russia's System of Operational-Investigatory Measures (SORM) that mandates a government eavesdropping capability. These include providing

virtual private networks (VPNs) for activists such as in China or Iran. To be sure, these efforts will threaten authoritarian regimes and feed their view of democracies as information aggressors; however, they hold and propagate this view regardless of democracies' actions. In choosing when and where to apply this policy, democracies should not ignore the potential for authoritarian backlash—including with narratives that paint democracies as aggressors that weaponize information to advance their interests and engage in the same behaviour authoritarians do. Ultimately, when calculating foreign policy actions and interests, democracies will need to weigh the downsides of this backlash with the potential gains from stemming the flow of information control technology and tactics. And to blunt the effectiveness of this authoritarian messaging, these "freedom of information operations" need to be truthful and transparent, refrain from manipulation, be conducted by democratic governments or civil society organizations, and include their own coordinated messaging component when appropriate. In short, they should serve as a clear contrast to the ways authoritarian regimes engage in information manipulation. While engaging in the same types of operations as authoritarian states is a losing proposition for democracies, a blanket unwillingness to challenge authoritarian information control implicitly condones it and allows for its spread.

(c) **Design And Promote Information Architecture And Governance Consistent With Democratic Values**. Finally, democracies should recognize that competing on message alone is not sufficient. The arenas in which the modern information contest plays out increasingly involve the

architecture of the information space itself and the norms governing it. In addition to the online information platforms addressed here, these architecture and governance dimensions include the physical network infrastructure that carries information, the international technical standards organizations that make decisions on global information technology requirements, the public and private surveillance systems that connect homes and cities, and the multilateral bodies and frameworks that govern the rules of these devices and the broader internet. In recent years, democracies have been largely absent from normative input into all of them. By contrast, China in particular has recognized the importance of this architecture layer in the broader information contest and is harnessing its state-driven private sector to set global technology standards. Democracies need to provide an attractive counteroffer to the authoritarian model, both for themselves and for less-consolidated democracies. This counteroffer could be provided through methods such as arguing for robust lawful access and data protection provisions in information systems, enacting strong data privacy legislation, competing in standards-setting organizations to build out the internet architecture of the future, and developing and championing ethical frameworks on AI bias, transparency, and accountability. Building positive, multilateral frameworks for the ethical application of information-driven technologies would put needed rhetorical distance between how democracies and authoritarian regimes use them while steering their use in a direction that protects democratic values, affirms the positive role of information in society, and rejects authoritarian misuse.

Who Should Lead Democracies' Efforts to Contest the Information Space?

20. Once democracies have determined how to approach the information contest, they need to determine who is leading the fight. **While the control and oversight will always be civilian there can be various models which can be adopted.** The information contest spans governments' defence, domestic and foreign policy institutions. Most democratic governments have no single actor with responsibility for either analyzing the information space holistically or coordinating democracies' defence or engagement in it. As Stanford researcher Herb Lin has detailed, fourteen US government agencies touch some aspect of the information contest. Yet democracies are not well resourced or structured to confront the challenge. To successfully contest the information space, someone needs to be in charge. But this is not an area where government is the primary actor, since much of the contest takes place on private playing fields. And authoritarian regimes can leverage their private sectors in ways democracies cannot and should not. Contesting the information domain will require innovation and nimbleness in approach, analysis of which roles are appropriate for government, and leadership from and coordination with the private sector and civil society. Democracies need new structures, modes of operation, and means of collaboration. Two options emerge with respect to the lead ministry/department.

21. Option I : Civilian Led. Issues and arguments which point towards a Civilian led Information contest structure are as follows (Laura Rosenberger and Lindsay Gorman, 2020) :-

(a) It can be argued that a democratic approach to the information contest must be civilian-led. Information warfare activities from authoritarian states often include significant military and intelligence components, and there is temptation to mirror this approach in response. But the targets of information manipulation are largely civilian, and the battle surface largely non-military. If protecting and advancing an information environment defined by democratic values is the goal, a military-led approach that weaponizes information undermines this objective. Democratic governments, therefore, should identify a civilian entity responsible for coordinating their engagement in the information space, in line with the principles articulated above. Crucially, this entity should not be authorized to remove content and must recognize the limitations of governments as direct messengers while empowering outside voices that promote quality information. Two examples from Europe present building blocks for democracies in forming and directing such an approach. The French government responded to a 2017 disinformation attack by creating a taskforce representing Foreign and Defence Ministries as well as academic and civil society groups. It shared lessons learned publicly, including that reporting on hacks before the disclosure of stolen documents helped inoculate voters. In Sweden, the government has distributed leaflets on disinformation and trained thousands of civil service employees, political parties, and journalists to identify foreign influence campaigns. It also constructed a dedicated line of communication with Facebook, Twitter, and Google to allow government officials to report fake pages and accounts. While not exhaustive, these efforts notably recognize the societal element of the information contest and crucially its non-military dimensions.

(b) A civilian-led approach will need to put coordination with online information platforms at the centre of its mission. This coordination will require government to be more transparent in sharing information with private companies and provide assessments of the strategic information environment and particular threat actors. The European Union's Code of Practice on Disinformation represents a first step in building a common public-private understanding on threats and remediation measures, even if its self-regulatory approach falls short. In the United States, a provision to establish a Social Media Data Analysis Center that would facilitate such sharing was included in the 2020 National Defense Authorization Act, though it has yet to be implemented. Ensuring appropriate protections for privacy and speech in this process will be critical to upholding civil liberties.

(c) A civilian-led approach will need to be supported by robust and holistic assessments of the information environment. This support will require coordination among the intelligence community, private sector, and civil society. For example, since 2016, the Estonian Foreign Intelligence Service has released an annual report to the public assessing the threat of Russian aggression and influence in Europe. The reporting is part of an ongoing effort to enhance public communication and government accountability necessary to build resilience across society.

(d) Military would have a limited part to play. Militaries would build information environment awareness around traditional battlespaces and

recognize that, in a permanent information contest, military operations themselves have a signalling effect that requires prioritizing the information component of an operation. For example, the lack of a coordinated information strategy around the US strike on IRGC Commander Qassem Solemani—including a delay in acknowledging the US role and mixed messages on the rationale—undercut any signalling effect to both adversaries and allies that the United States may have intended and created a vacuum for US adversaries to fill. Militaries would also continue to engage in limited offensive cyber operations, including on the infrastructure supporting adversaries' information operations and the forward defence of democratic information networks from compromise. For example, in advance of the 2018 US midterm elections, US CYBERCOM reportedly pre-emptively and temporarily disrupted the internet access of Russia's Internet Research Agency out of concern for influence attempts.

(e) Civil society would analyze and monitor the information domain, especially domestically, where democratic governments face limitations on surveiling their own populations. Due to their independent credibility, civil society actors will often be the best sources for public-facing analysis of the information environment. The public and private sectors thus need robust means for cooperating with civil society while maintaining its independence. In the Baltic states, for example, groups of volunteer internet users known as "elves" work to debunk pro-Kremlin disinformation narratives by pushing out information from reliable sources. A strong civil society is also important to

holding governments and the private sector accountable to the principles outlined above. The ability to bring to bear disparate, vibrant sectors of democratic society is vital to democracies' success in the information contest and to their global offering. This would also apply to a Military- Led contest of the information space.

22. **<u>Option II : Military Led</u>**. Issues and arguments which point towards a Military led Information contest structure are as follows :-

(a) The aspect of dominating the Information domain both in terms of defending against disinformation and configuring and executing SCEIIO is primarily a national security construct. While it can be controlled through the NSC, the lead must be with the MoD/Defence Forces with suitable interagency coordination.

(b) Major thrustlines connected to Information Operations are being led or being planned to be led by the Defence Forces. The SSF in China has aggregated every aspect of information operations and is under the direct control of the CMC. UK has the 6 Division carrying out this exclusive role. The US CYBERCOM led the endeavour to ensure that the US Elections are not interfered with both in 2018 midterms and in 2020 Presidentials. There is a thought process to re-christen the US Army Cyber Command as an Information Warfare Command as SCEIIO appears to have become a primary line of effort. The US CYBERCOM is also likely to follow this change in nomenclature to reflect its major focus.

(c) While defensive measures and a whole of government and nation approach is key to countering disinformation the more offensive aspect of SCEIIO to include proactive operations to disrupt adversary SCEIIO infrastructure would be best planned and executed by Defence Forces. This is evident in the “Defend Forward” and “ Persistent Engagement” strategy of US CYBERCOM.

(d) As large scale conventional conflicts take a backseat and are being largely replaced by a perpetual and seamless continuum of peace-short of war competition, Non Contact Warfare assumes pole position. Shaping operations in the form of Non-Kinetic, Non Contact Warfare through SCEIIO assumes significance and would have to be informed by a National Information Security Strategy which in turn would be a derivative of a National Security Strategy. Hence, this effort towards Influence operations would have to be wide spectrum both in terms of addressing all countries impacting the security dynamics of a nation and being prosecuted across the entire peace-war continuum. Consequently, they would be helmed by the apex national security body and should ideally be led by Defence Forces.

(e) Organizational capacity to undertake SCEIIO at the desired scale and effect may not be feasible within MEA or MHA or an Intelligence Agency. While some quarters in USA had suggested DHS (MHA equivalent) or enhancing the existing GEC within the Department of State and in UK MI 5 (UK, House of Commons, 2020), more pointedly for Countering Disinformation, for the entire package of wholesome SCEIIO, capacities may only exist with the Cyber/Information Operations organizations of the Defence

Forces to lead the effort. Ben Hatch cites "Thomas Hill, a former House senior staffer, "If people were serious about combating Russian propaganda, you have to be honest -- $80 million and 50 people in the basement of the State Department [are] not going to cut it. That is not enough." A January 2018 U.S. Senate report specified, "In early 2017, Congress provided the State Departments [GEC] the resources and mandate to address the Kremlin disinformation campaigns, but operations have been stymied by the Department's hiring freeze and unnecessarily long delays by its senior leadership in transferring authorized funds to the office." In April 2018, a U.S. Combatant Command senior representative engaged in information operations said he was unaware of any GEC messaging efforts, pithily stating, "They ain't talking to us." Another official familiar with the GEC's efforts in Europe's Black Sea Region described them in terms that were limited in scope to ensuring that ongoing individual U.S. government efforts were complementary." **Consequently, the GEC may not be a suitable option to oversee strategic information operations without significant additional investments. Therefore, assigning the lead for strategic information and cyber-enabled information operations within the DoD may be a more attractive alternative."**

(f) Hillary Clinton while advising Richard Stengel heading the GEC, as she was leaving, opined that " ….you would be obstructed by Public Affairs (under State Department) as I was - they are too cautious and too afraid of making mistakes. We need to do much more and you cannot let the old ways of doing things stand in your way." **She added that the Defense Department**

and the intelligence community would be better partners for both counter- Russian and ISIS messaging (Richard Stengel, 2019).

(g) Lt Gen RS Panwar (Retd), ex Indian Army, has argued, "***Armed Forces as Pivot for CIO*** **-** At the outset, it may be stated that no Cyber Influence Operations (CIO) doctrine appears to have been enunciated by any nation so far, and CIO remains a nebulous concept at this juncture. Notwithstanding this, due to the increasing employment of CIO by nations in recent years for achieving strategic effects, it is an imperative for India to formalize an approach in this area and develop capabilities accordingly. …….. it is fairly evident that any structural model for conduct of CIO would involve the use of non-military resources to some extent (news media for PA, non-state actors for troll armies, etc). Notwithstanding this, the overriding consideration while arriving at such a model is that CIO be considered as an essential component of an overarching Armed Forces strategy for multi-domain operations (MDO) across the entire spectrum of conflict. Moreover, the author has argued elsewhere that the Armed Forces must have the sole charter for the defence of our national cyberspace, and particularly for the conduct of offensive cyber operations. Since CIO play out in cyberspace and need intrusive CO for achieving their full potential, the Armed Forces are the logical choice to act as a pivot for operationalizing this concept, with issuance of doctrines as a first step."

(h) Another important way to arrive at a lead department/organization/agency is to see this issue through the prism of a 'Global Common'. Other global commons like the Seas, Air and Space, while

being extensively used by the private/civil sector based on international treaties/laws, are provided security by the respective Defence Forces. The Information Environment which largely encapsulates Cyberspace - the only man-made global common - and where laws/norms are still not crystallised, must therefore be defended with the Defence Forces in lead.

(i) Indian Defence Forces have been dealing with IW/IO for almost two decades now. They have published Service level and Joint IW Doctrines. The Services have individual IW Training Schools e.g. the Indian Army runs IW Courses at the Army War College and the IW Vertical is manned down till the Corps HQ level. As part of a recent upgradation at the Army Headquarters a new post of DG IW has been created. The Navy and Airforce too are aligned on similar lines. Hence, this legacy expertise with the Defence Forces possesses the necessary capacity and direction to expand and extrapolate to the National Level effectively and seamlessly.

Organization/ Interagency Coordination Issues

23. The effectiveness of a government's information capabilities is a reflection of how it is organized. The United States Government (USG) and DoD oftentimes struggle to organize for information and cyber-enabled information campaigns that would afford decision makers flexible options to advance and defend political ideals. Frequently, the USG holds its vast information capabilities in uncoordinated stovepipes, and misses potential strategic advantages gained through combined action, unity of command, and unity of effort. Russia has overcome these organizational barriers, and according to RAND analyst Bruce McClintock, "The Russian

information operations system, combined with the Russian form of centralized government control, allows it to launch cyber-operations with greater speed, agility, and brazenness than most analysts believe is possible in the West."

24. History illustrates the value of an organized capability to conduct and defend against strategic information operations. The British during World War II established an organization for controlling the dissemination of specific information to the Germans. The design of the British system included centralized control of the strategic influence initiative focusing on the employment of turned foreign agents and other human sources. According to J.C. Masterman, the W. Board, comprised of Britain's senior leaders, specifically the three directors of intelligence, Chief of the Security Service, and the head of the B. Division in M.I.5 (similar to the U.S. Federal Bureau of Investigations), oversaw the strategic direction of plans and operations using agents as information pathways to deliver select messages to desired recipients. Subordinate to the W. Board, the Twenty Committee (XX Committee) oversaw the general day-to-day management of the specific operations, and became the focal point for all information transmitted to the enemy. Masterman stressed that the British successfully used this system to integrate and synchronize information used to steer German thinking and behaviour in part because there was a section dedicated to the special work**. In other words, there was centralized control of the system, but also decentralized execution through multiple departments. Such a model highlights that a government's ability to engage in strategic information operations is most successful when there is an integrated organizational and operational construct, with access to strategic levels of government, to manage influence operations**

conducted across multiple agencies, departments, and domains (Ben Hatch, 2019).

25. More recently, there have been isolated attempts within the U.S. Defense Department to posture organizational resources to fight effectively in the information domain. For example, in the global conflict against the Islamic State, one combatant command implemented a reorganization to integrate and synchronize lethal and non-lethal effects, notably by aligning Information Related Capabilities (IRCs) previously located and managed by leaders in their J2, J3, and J6 offices under a single advocate for information operations in the operations division (J3). A senior defense official noted, "We must be organized properly" to be effective at information operations. This example shows that organization was the solution to harmonize the effects of multiple strategic communication tools found in otherwise disjointed and stove-piped IRCs. The British, Soviet experiences, and the Islamic State example illustrate that strategic information operations are more successful when an organization dedicated to information related activities, both offensive and defensive, is responsible for management and oversight of the operations. The World War II and Cold War examples show that when centrally managed, information operations inform and shape specific audience perceptions in order to gain a competitive advantage. **The United States presently lacks a unified framework to identify, defend, counter, integrate, and synchronize its available information capabilities for multi domain operations, and it should consider a new organizational construct to address these challenges in the future (**Ben Hatch, 2019**).**

26. **A leading organizational proposal** under consideration is the creation of a National Information Office. In testimony to the Senate Armed Service committee,

The Honorable Michael D. Lumpkin, former Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD/SOLIC), argued the merits for creating a national information office. He considered a model for the office advocated for by former Director of National Intelligence James Clapper, which was the resurrection of the now defunct United States Information Agency (USIA), although Director Clapper opined the re-established USIA would need to be more robust based on the emerging information landscape. While agreeing there would be benefits with reconstituting the USIA, Lumpkin acknowledged there were also challenges and other issues that led to its disestablishment. Instead of the USIA, Lumpkin argued for elevating the U.S. State Department's Global Engagement Center (GEC) to a position similar in status to the Director of National Intelligence. In doing so, it would align authority, responsibility, and accountability for information operations under a single office, and a single information strategy. At present, the GEC, charged with "leading the USG's efforts to counter propaganda and disinformation from international terrorist organizations and foreign countries," has limited resources and capacity (Ben Hatch, 2019).

Beyond the Govt

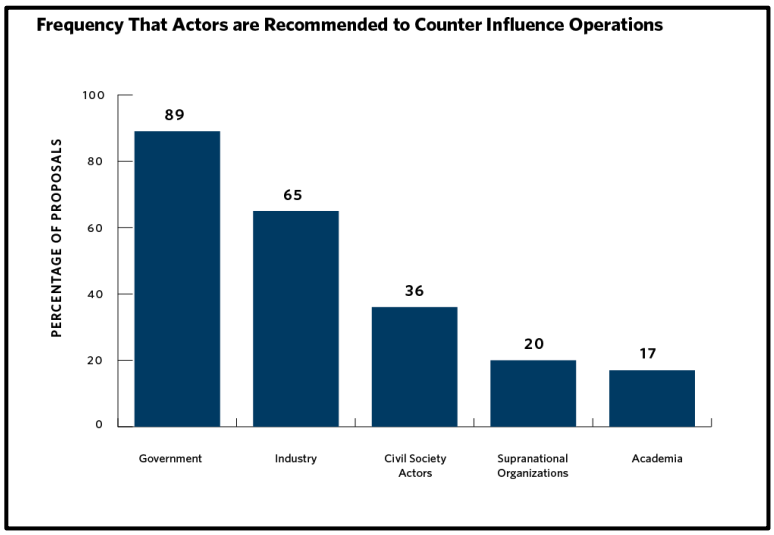


Figure 5.1 – Frequency that Actors are Recommended to Counter Influence Operations

27. The Partnership for Countering Influence operations (PCIO) has reviewed eighty-four papers published since 2016 that offered policy recommendations for countering influence operations. These came from fifty-one think-tanks, academic institutions, and government strategic communication organizations in North America and Western Europe. The review suggests that existing policy recommendations on countering influence operations have set a general course for policymakers and laid the foundation for future research. The vast majority of publications in the data set addressed recommendations to governments (89 percent) and industry actors (65 percent). In contrast, civil society actors, supranational organizations (such as NATO), and academic institutions were less frequently mentioned (see **Figure 5.1**). Researchers seem to expect governments and companies, particularly social media platforms, to lead the charge against influence operations. This makes sense: governments and platforms have more resources, unique access to data, and the capability to intervene directly against influence operations.

28. However, other institutions also have critical roles to play and deserve more attention. Civil society is integral to media literacy, fact-checking, and independent journalism, for example—all areas widely recognized as crucial for combating influence operations over the long term. Academics can help to measure the actual impact of influence operations and the effectiveness of countermeasures—which, perhaps surprisingly, are largely unknown today and represent major barriers to policy progress. Supranational organizations can coordinate efforts across national governments and set up regional countermeasures against influence operations. As researchers continue to focus on what governments and platforms can do right now, they should not neglect other actors that are essential for long-term, whole-of-society solutions (Kamya Yadav, 2020).

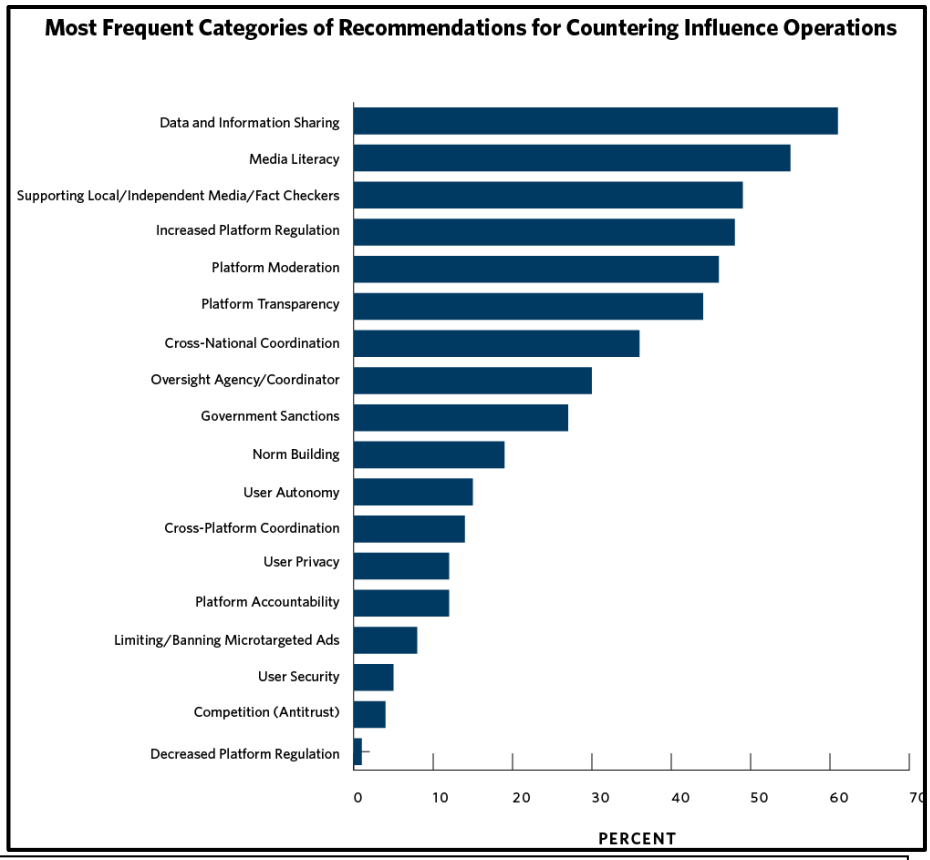


Figure 5.2 – Recommendations for Countering Influence Operations

29. **Policy Areas**. Recommendations covered a broad range of policy areas, with some areas receiving much more discussion than others (see **Figure 5.2**) The most common categories for recommendations were: sharing more information and data (by governments and social media platforms), fostering safer media environments (through media literacy and supporting local or independent media), and enacting new rules or practices for platforms (via government regulation, content moderation rules, and greater transparency). The focus on these areas suggests an emerging consensus among experts that they represent the most urgent priorities for policymakers.

30. The first edition of "*Democratic Defense Against Disinformation (Daniel Fried & Alina Polyakova, 2018"* offered recommendations on ways democratic governments and free societies can combat disinformation, while respecting the norms and values of free expression and the rule of law. As democratic countries learned in

the struggle against Soviet communism, they need not become them to fight them: democratic societies should not fight propaganda with propaganda, nor should they turn to censorship. Freedom of expression and US First Amendment protections do not rob free societies of options. US law prohibits foreign participation in US elections, broadly defined, and permits extensive regulation of commercial advertisements (e.g., outright bans on broad categories, such as smoking). In general, foreign persons, especially outside the United States, do not enjoy full First Amendment protections. Automated (e.g., bot) social media accounts also do not necessarily have First Amendment rights. EU/European options are still broader and include legal and regulatory options for enforcing versions of media fairness and impartiality. And, in some countries this includes authority to ban certain forms of hate speech, though this has drawbacks. This paper's initial recommendations covered three levels of action, summarized below:

(a) **Governments**. Starting with the United States, European national governments, the EU, and NATO, should introduce and enforce transparency standards, including with respect to foreign-origin political and issue ads on both traditional and social media, and otherwise monitor and notify their publics in real time about the activities of foreign propaganda outlets. To that end, governments should establish "rapid-response task forces" to inform government officials and, as needed, allies, of emerging disinformation campaigns that threaten national security. Governments should also expand institutional capacity, building on the EU's East StratCom, NATO's StratCom Center of Excellence in Riga, the Helsinki Hybrid Center of Excellence, the Department of Homeland Security's task force to counter malign foreign

influence, and the US State Department's Global Engagement Center (GEC), to identify and expose Russian and other disinformation campaigns.

(b) **Social Media Companies**. Have a responsibility to stop denying and start mitigating the problem of foreign disinformation. The paper specified that they should: identify and label overt foreign propaganda outlets (RT and Sputnik, for example) as state-sponsored content; experiment with labelling and taking down automated and fake accounts; and redesign algorithms to demote, de-rank, or mute known propaganda content and suspect or misla-belled content, based on findings from third-party fact checkers.

(c) **Civil Society Groups**. Especially the tech-savvy "digital Sherlocks" skilled at identifying disinformation—such as Ukraine's StopFake, Bellingcat, the Atlantic Council's Digital Forensic Research Lab, the Alliance for Security Democracy's Hamilton , EU DisinfoLab, and the Baltic Elves—have proven skilled at identifying coordinated disinformation activity driven by inauthentic accounts, often in real time. They, and other innovative startups, are better able than governments to develop the tools to identify emerging disinformation techniques (e.g., synthetic media and deepfakes). Governments, social media companies, and philanthropic organizations should fund such innovators and establish regular lines of communication with them, e.g., through designated points of contact.

Imperatives for National Structures in India for SCEIIO

31. Creation of or reorientation of existing organizations to arrive at an effective and appropriate structures for planning and conduct of Information Operations/SCEIIO would be driven by certain imperatives which are as follows:-

(a) **Whole of Nation Approach**. Strategic Information Operations especially SCEIIO merit a "Whole of Nation Approach". With exponential increase in internet penetration expected in the next five years the ability of an adversary to influence chosen sections of populace is a potent threat. Or stove-piped actions therefore will not yield the desired results. Defending against disinformation would start from the civil society and end at the apex national security bodies.

(b) **Balanced Defensive- Offensive Nature**. While a substantial effort of SCEIIO would be defensive in nature to counter adversary influence activity, intrinsic to this defensive activity would be strong offensive/ proactive defensive measures. Also, India must not hesitate in prosecuting meaningful and appropriate SCEIIO against her adversaries to dominate proactively and shape adversary information space favourably. Importantly, it must be understood that "Active Defence" would yield the best results and therefore actions may predominantly have to be proactive and offensive in nature. The national structures must reflect such a balance.

(c) **Peace – War Continuum**. The prosecution of SCEIIO would not just be limited to a pre-conflict and conflict period. It will span the entire Peace-War continuum in a persistent manner. Therefore part-time or dual tasked organizational structures may not be the answer.

(d) **Cyber Technical & Information Operations Synergy**. While these operations differ in substance and effect they have overlaps and symbiotic connections. It may therefore be appropriate to co-structure organizations tasked to carry out these operations. Classic Cyber Security organizations with a completely defensive mandate, however, may be kept outside these structures. As brought out before, the convergence of "Information Warfare Elements" is already catalysing a move towards analogous convergence of organizations which is being reflected in proposed rechristening of "Cyber" to "Information" Operations structures.

(e) **Strategic Synergy with all Elements of National Power**. The structures must manifest strategic synergy across all organs of governance and be helmed by the apex national security body to synchronize SCEIIO efforts effectively.

(f) **Centralised Planning & Decentralised Execution**.The nature of social media and the speed and intensity of narratives that can impact SCEIIO merits that execution of the same is highly decentralised. Hence, while campaigns maybe planned at the highest level, day to day execution and control must be decentralised.

(g) **Borrowing from Global Models**. Global models of Information Operations' organizations reflect a heavy leaning towards Military/Defence Organizations. While defensive cyber security for critical infrastructure is based in civilian organizations, offensive Information or Cyber Operations are largely the preserve of Defence Forces. However, this canvas needs to be enlarged to carry out meaningful and potent SCEIIO. Both US CYBERCOM and Chinese SSF encapsulate a major proportion of capacities of their respective nations for prosecuting SCEIIO and can be borrowed from.

(h) **Configuring & Publishing Information Operations Strategy/Doctrine**. While a National Cyber Security Strategy is under formulation under the NSCS, there is a need to configure a National Information Security Strategy which can feed into a Joint Information Operations Doctrine for the Defence Forces. These formulations will inform the structural changes or raisings required to be implemented.

(i) **Upscale / Reorient Defence Forces' Cyber/Information Operations Organizations**. There is a clear requirement to upscale the existing Defence Organizations handling Cyber/Information Operations. The DCyA must be upscaled to a full fledged Command. DIARA had converted to DCyA and is therefore best suited to be the Apex organization for planning and conduct of SCEIIO at the Tri- Service level. Accordingly, it could be rechristened as Defence Information Operations Command and would be the single point contact with the NSCS for SCEIIO efforts at the National level.

With the upscaled capacity, it could house the National Information Operations Command Post as the unified and single point locus of all SCEIIO efforts.

(j) **Counter Terrorism Related SCEIIO**. India has a major stake in Counter-Terrorism and SCEIIO connected to this domain would have to be prosecuted in perpetuity. With J & K, North-East and patches of LWE, Counter Terrorism related SCEIIO would merit special attention. Joint Task Force ARES created by the US CYBERCOM to fight ISIS in the Information space is a good example.

(k) **Securing Elections**. Malign Interference in elections and referendums through social media platforms has been a major cause of concern as it strikes at the very core of democratic processes. There have been clearly discernible instances of such interferences in US & Taiwan elections as well as the Brexit referendum. India too may be subjected to such interference given the scale of elections and diversity of issues. From creating Election Observation Missions by EU to Task Forces by USA have been specially tasked to ensure the security of elections.

(l) **Institute a formal mechanism for information-sharing that includes key players from the government and private social media companies.** While social media companies have control over their platforms, with an ability to filter out or identify suspect accounts and content, the government often has superior information about adversary strategies, tactics,

and adaptations. A formal mechanism for information-sharing would enable social media companies to implement measures earlier, rather than after the execution of a particular influence operation, facilitating both the detection and curtailing of adversary proxies and the reduction of potential amplification channels. Anonymized social media data would enable government organizations to connect trends to specific disinformation tactics, techniques, procedures, and adversary groups, while tips from those same organizations could help social media companies detect and remove disinformation early. The specific mechanism could take different forms, but at minimum should consist of a standing committee with participants from social media companies, government organizations, the intelligence community, NGOs, and academia.

(m) **Increase The Transparency of Social Media Platform Policies and Algorithms for Detecting and Removing Disinformation and Malicious Behaviour.** Social media companies are currently facing pushback from both consumers and government organizations for the role their platforms have played in the spread of disinformation. Increasing the transparency of their algorithms and policies for what content constitutes disinformation, what behaviours violate terms of service agreements, and how content and accounts are demoted or removed will increase consumer confidence in these platforms and potentially pre-empt the passage of more heavy-handed legislative or regulatory efforts to combat the influence operations/disinformation threat. A key aspect of transparency is enabling outside observers to verify and validate the approaches technology companies are taking to reduce disinformation—

without this increased insight, it would be impossible to know whether private companies are making any difference. A Social Media Data Analysis Centre and a Rapid Alert System (on the lines of EU) can provide the necessary impetus.

(n) **Encourage and Fund Academia to Develop Better Tools for Identifying and Attributing Disinformation on Social Media.** Increased transparency of algorithms and data will also enable academic researchers to develop better tools for the identification and, most importantly, attribution of disinformation and malicious actors on social media. Together with increased funding from various non- government foundations and government organizations, this approach can improve the ability of individuals and platforms to identify disinformation.

(o) **International Synergies**. It is important that linkages are created with like minded nations especially democracies on countering Disinformation through SCEIIO. USA, UK, EU and NATO must be engaged and a partnership of democracies can be configured solely for this purpose on the lines of the intelligence coalition of " Five Eyes" or "D 10" a coalition of 10 Democracies, as advocated by UK for an alternate to the Chinese 5G technology domination .

(p) **Legal Initiatives**. It is important that key legal reforms connected to data privacy and protection of print and electronic media through revenue sharing with social media platforms, among many others, are enacted. While

EUs GDPR was a lead in data privacy and protection, the recent initiative by Australia to share revenue from news between social media platforms and Media Houses are key steps to curb Disinformation. The recent guidelines issued for social media platforms in India is a step in the right direction.

(q) **Regulation of Social Media Platforms – Intermediaries Issue**. Social media has opened up new channels of communications but the degree of decentralization of transmission of information means the extent to which state can regulate has further decreased. Most importantly, social media platforms being treated as intermediaries for news absolves them of any responsibility for the content that pervades their platforms. This needs to be changed. The era of Post – Truth has been catalyzed by propaganda and disinformation on social media which can erode democratic processes, create racial or ethnic tensions, support the rise of an organization like Daesh/ISIS and cultivate an Arab Spring. A single tweet can be a story. Disinformation and divisive terror inclined propaganda therefore needs to be called out through regulation. Lastly, personal data being collected by these platforms , apart from being exploited for targeted ads can be weaponized for micro-targeted influence operations. Monetization of personal data for any reason needs regulation.Regulation must not intrinsically intrude on the creative or business models of these platforms. It must however ensure that personal data protection, national security issues, disinformation and responsibility for news content are brought within the ambit of regulation.

32. Keeping in view the above imperatives, a recommended structure is shown below :-

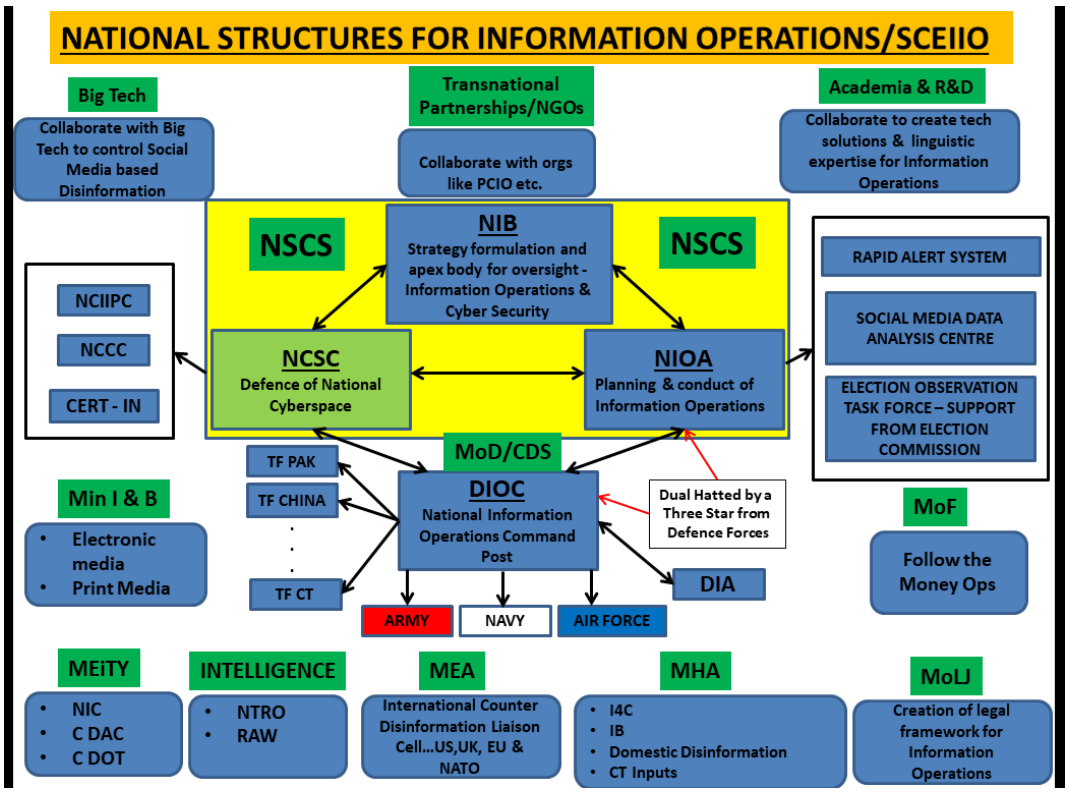


Figure 5.3 – Recommended National Organizational Structures for Information Operations/SCEIIO Operations

Legend

NIB – National Information Board

NCSC – National Cyber Security Coordinator

NIOA – National Information Operations Agency

DIOC – Defence Information Operations Command

NCIIPC – National Critical Information Infrastructure Protection Centre

NCCC – National Cyber Coordination Centre

DIA – Defence Intelligence Agency

TF – Task Force

(a) **Apex Bodies**. The apex bodies within the National Security Council Secretariat are as follows :-

(i) **National Information Board (NIB)**. This is the highest body dealing largely with cyber security issues presently and is headed by the NSA. Information Operations Strategy formulation at the national level and necessary oversight will have to be exercised by this Board as a fresh mandate.

(ii) **National Information Operations Agency (NIOA)**. This agency would be mandated to plan and conduct Information Operations at the National Level. Its manning should be largely from Defence Forces and Domain Specialists from other govt organizations/private sector. Its mandate for execution, however, would be more defensive in nature focusing more on "Countering Disinformation". The "influence" and "shaping" part of Information Operations would be undertaken by DIOC. It could have the following TF/platforms :-

(aa) **Rapid Alert System**. On the lines of EU, this technical platform, suitably manned would encapsulate speedy discernment of all possible lines of efforts of adversary disinformation, dissemination to all concerned and maintain intimate connectivity with friendly foreign systems of similar hue.

(ab) **Social Media Data Analysis Centre**. The ubiquitous nature of social media platforms and Disinformation primarily being vectored through these platforms, continuous data analysis to predict and trap malign activity pointing towards adversary SCEIIO is absolutely essential.

(ac) **Election Observation Task Force**. Lately, major global disinformation and influence campaigns have targeted elections in democracies. SCEIIO based election interference can have serious setbacks during and beyond the elections and jeopardize this core democratic process. With elections being held frequently in India, it is important that task forces monitor closely any attempt to poison the electoral process and where feasible take proactive measures to neutralize such threats. This would be supported by the Election Commission.

(iii) **National Cyber Security Coordinator (NCSC)**. This office will continue with its role of ensuring the security of national cyberspace with the National Critical Information Infrastructure Protection Centre (NCIIPC), National Cyber Coordination Centre (NCCC) and CERT-In reporting to it. However, SCEIIO can be preceded by or run in parallel with cyberspace hacks which compromise individual targets or entire networks. Hence, intimate operational synergy would be needed between NIOA and the NCSC.

(b) **Defence Information Operations Command (DIOC)**. DCyA alongwith Army, Air Force and Navy Cyber Groups was raised in 2019. DIARA converted to DCyA and therefore is ideally poised to be the apex Defence Forces' organization for planning and conduct of Information Operations both within the Defence Forces' domain as well as at the national level. At the national level, in concert with NIOA, it would primarily engage in disruption of adversary SCEIIO infrastructure connected to disinformation targeting India and execute shaping operations in the Information domain to support national security objectives. It will also continue to execute its mandate of protecting the Defence Cyberspace too. In line with all major cyber powers, it is important that DCyA is upscaled to a Command and suitably resourced and staffed. In order to reflect its role and mandate it could be re-christened as the Defence Information Operations Command wherein, Information Operations would subsume Cyberspace & Cyber Enabled Influence Operations. Two important measures would impart the necessary fusion and synergy and ensure a Defence – Offence continuum for SCEIIO at the National level as well as break down Defence-Civil silos in this field as propounded by the Hon'ble Prime Minister during the recent Combined Commander's Conference in Kevadia viz. Dual hatting of NIOA and DIOC by a Three-Star Officer from the Defence Forces and housing the National Information Operations Command Post within the DIOC. The dual hatting would also ensure unity in Command of two organizations handling the Defense and Offense spectrum of Information Operations as these operations are inextricably linked. It will also ensure optimization of national resources and the workforce and provide a fillip of scales as the cumulative potential of

these two organizations is harnessed under a single head. A task force based sub-structure has been recommended to ensure greater focus.

(c) **Ministries/Intelligence Agencies Representation**. As shown above concerned ministries would have to create special contact points/ cells to contribute to the national effort of conduct of Information Operations. The role of MEA and MHA would be critical in terms of international connectivities and messaging and handling domestic disinformation, respectively. Adversaries have been known to discern instances of domestic disinformation and amplify them based on their specific requirement. Defence against such domestic cases would be best dealt under the aegis of MHA with suitable assistance being provided by DIOC, if required. Both RAW and NTRO would be able to provide the requisite inputs to NIOA-DIOC.

(d) **Big Tech Collaboration**. Since a major portion of SCEIIO is across Twitter, Facebook and Youtube, it is key that NIOA has a mandate to collaborate directly with these and other platforms to create suitable and appropriate regulatory and monitoring mechanisms without impacting privacy and free speech.

(e) **Transnational Partnerships/NGOs**. India must take a lead in establishing coalitions of like-minded nations for joint messaging/SCEIIO especially connected to terrorism and plug into existing ones. The Joint UAE - USA Anti ISIS Messaging Centre also called the “Sawab Centre” (Sawab-Right Way) in Abu Dhabi is a good example of such an initiative which can be expanded. There is also a need to plug into transnational non-government initiatives like Partnership for Countering Influence Operations (PCIO) and

similar initiatives. It may be worthwhile to fund an Indian Think Tank to venture into this field.

(f) **Academia and R&D**. AI based tools both for defence and offensive actions like Disinformation toolkits, Disinformation defence tools, Deep Fakes, etc. is going to revolutionize SCEIIO. Both academia and R&D agencies need to be engaged to address this field suitably and create indigenous solutions/ tools for society at large and niche products for NIOA-DCIO. The School of Foreign Languages must develop bespoke programmes for ensuring linguistic expertise. The American GEC realized the importance of linguistic skills in Arabic and Russian. Less than ten percent of ISIS messaging was in English; most of it was in Arabic. Similarly, looking at our adversaries, Chinese and Pakistani language proficiency is a must to conduct meaningful SCEIIO.

CONCLUSION

" The modern Internet is not just a network, but an ecosystem of nearly 4 billion souls, each with their own thoughts and aspirations, each capable of imprinting a tiny piece of themselves on the vast digital commons. They are the targets not of a single information war but of thousands and potentially millions of them. Those who can manipulate this swirling tide, to steer its direction and flow, can accomplish incredible good."

- ***PW Singer***

1. India sits on an 'Information Tinderbox' encapsulating the country's numerous faultlines reflected in failed insurgencies, a prolonged proxy war, the LWE internal security threat and a unique diversity being held together by a young but thriving democracy. Its civilizational soft power construct of "Vasudhaiva Kutambakam" , huge demographic dividend, economic potential and a strong military, places it at the cusp of global power status. What holds it from moving beyond this cusp are two adversaries who have leveraged land border disputes, are authoritarian states driven by outdated ideologies and are colluding to hem India into a regional power status. While Pakistan has exploited the Information Environment very recently to radicalize the youth in J & K, China's recent cyber attacks on Indian electricity grids and Vaccine companies point towards a period of intense Non-Contact Warfare, led by Information Operations.

2. It can be argued that unlike the USA and EU, India has still not experienced large scale Disinformation or classic SCEIIO till now. There have been no known instances of interference in our elections or any other democratic processes. This, however, is most likely by design and not by default. That is, it certainly is not due to lack of capacity of our adversaries. However, with a strong government at the Centre with a decisive electoral mandate, which has exercised unprecedented political will to take strong decisions in national interest like abrogation of Article 370 and the CAA Bill, amongst others, it could create potential surface areas for disinformation activity. The decision to build stronger relations with the US and promoting the QUAD for an open and free Indo-Pacific too is also creating tremors amongst regional adversaries. Coupled with this, an exponential internet penetration and the largest number of Facebook users in the world, India offers an attack surface both quantitatively and qualitatively ripe which can be exploited by our adversaries. Hence, there is a dire need to address this issue pro-actively backed by appropriate organizational structures, interagency coordination, international cooperation and legal regimes.

3. There are a few key issues which have emerged from this study. Firstly, there is a lack of doctrinal endeavours and terminology in this domain globally which must be addressed. Secondly, while influence operations/propaganda is not a new arrival its prosecution through cyberspace is, with massive ramifications on national security. Thirdly, Cyberspace Operations differ from Cyber Enabled Information Operations. They can be conflated but their organizational and skill requirements are different. Fourthly, like most democracies India has been reluctant to adopt Information Operations measures overtly. This has to change as our adversaries will exercise no such reluctance. Fifthly, SCEIIO has to have a whole of nation approach across the

entire peace-conflict continuum. It has to be strategic in nature, reach and outcomes. Fifthly, it must be centralized and apexed for planning & oversight at the NSC level. Sixthly, it must predominantly be led by the Defence Forces. Lastly, there must be synergy between SCEITO and SCEIIO organizations as these operations are symbiotic in nature.

4. Kautilya's Arthashastra mentions "Silent Wars" as one of the categories of war which requires stealth and classic non-military means to undermine the enemy. As the space for conventional conflict constricts, alternate domains like Cyberspace will offer opportunities to "Win Without Fighting" kinetically. India's massive digital footprint which promotes governance, the economy and education needs to be protected from this Non-Contact Warfare. While India has moved to address Cyberspace Security in right earnest and the impending National Cyber Security Strategy-2021 would further provide a fillip to it, protecting the nation's Cognitive Dimension nested within its Information Environment and exploiting the adversary's, requires a different set of doctrinal and organizational endeavours. The study recommends one such model derived through a scrutiny and analysis of global models.

REFERENCES

1. A Kiyuna & L Conyers, (2015). Cyberwarfare Sourcebook.

2. Alina Polyakova & Daniel Fried (2019). Democratic Defense Against Disinformation 2.0, Atlantic Council Eurasia Center.

3. Allcott, H., Gentzkow, M., (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspective, pp. 211 – 235.

4. Andrew Weisburd, Clint Watts and Jm Berger, (2016). Trolling For Trump: How Russia Is Trying To Destroy Our Democracy, War On The Rocks.

5. Arturo Munoz, (2012). U.S. Military Information Operations in Afghanistan

6. Baezner, M., Robin, P., (2017). Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict Version 2. Center for Security Studies (CSS), ETH Zürich, Zürich.

7. Ben Hatch (2019). The Future of Strategic Information and Cyber-Enabled Information Operations ,The Berkeley Electronic Press.

8. Blagovest Tashev, PhD; Lieutenant Colonel Michael Purcell (Ret); and Major Brian McLaughlin (Ret), (2019). Russia's Information Warfare Exploring the Cognitive Dimension , Marine Corps University Journal, 2019.

9. Blank, S., (2017). Cyber War and Information War à la Russe, in: Understanding Cyber Conflict: Fourteen Analogies. George Perkovich & Ariel E. Levite, Washington, DC, pp. 81 – 98.

10. Bonfanti, M., (2019). An Intelligence-based approach to countering social media influence operations, in: Romanian Intelligence Studies Review. National Intelligence Academy, Bucharest.

11. Brian Bartholomew & Juan Andres Guerrero-Saade, (2016). Wave Your False Flags! Deception Tactics Muddying Attribution In Targeted Attacks, Kaspersky Lab, USA.

12. Bright, J., (2016). Explaining the emergence of echo chambers on social media: the role of ideology and extremism. SSRN Electronic Journal.

13. Bruno Lupion (2019). EU Framework Against Disinformation, Democracy Reporting International.

14. Catherine A. Theohary**,** Specialist in National Security Policy, Cyber and Information Operations,(2018). Information Warfare: Issues for Congress Congressional Research Service,Centre of Excellence.

15. Christopher Balding & Robert Potter (2020). Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua .

16. Cohen, D., Bar'el, O., (2017). The Use of Cyberwarfare in Influence Operations. Tel Aviv university.

17. Colonel Anurag Dwivedi (2019). Modern Information Warfare.

18. Credible Cyber Deterrence in Indian Armed Forces (2019). VIF

19. Cronin, B., Crawford, H., (1999). Information Warfare: Its Application in Military and Civilian Contexts. The Information Society, pp. 257 – 263.

20. Cronin, B., Crawford, H., (1999). Information Warfare: Its Application in Military and Civilian Contexts. The Information Society, pp. 257 – 263.

21. Daniel Kliman, Andrea Kendall-Taylor, Kristine Lee, Joshua Fitt, and Carisa Nietsche , (2020). Dangerous Synergies - Countering Chinese and Russian Digital Influence Operations, CNAS.

22. David Patrikarakos, (2017). War in 140 Characters – How Social Media is Reshaping Conflict in the Twenty First Century.

23. David Sanger & Emily Schmall, (2021). China Appears To Warn India : Push Too Hard And The Lights Will Go Out, New York Times.

24. DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J., Johnson, B., (2018). The Tactics & Tropes of the Internet Research Agency, New knowledge.

25. Dorothy E, (2011). Cyber Conflict as an Emergent Social Phenomenon Denning, Calhoun Naval Post Graduate School.

26. Douglas Walton, (1997). What Is Propaganda, and What Exactly Is Wrong with It? , University of Windsor.

27. Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, Elina Treyger, (2018). Countering Russian Social Media Influence, RAND.

28. Elsa B Kania & John K Costello(2018). Strategic Support Force and the Future of Chinese Information Operations.

29. Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, Cathryn Quantic Thurston-RAND (2009). Foundations of Effective Influence Operations

30. Hearing Before The Subcommittee On Cybersecurity Of The Committee On Armed Services United States Senate One Hundred Fifteenth Congress First Session April 27, 2017. Cyber–Enabled Information Operations.

31. Herbert Lin (2019). The Existential Threat From Cyber-Enabled Information Warfare.

32. Herring, S., (2002). Searching for Safety Online: Managing 'Trolling' in a Feminist Forum. The Information Society. pp. 371 – 384.

33. Iain King, (2020). Towards An Information War Theory Of Victory, Modern War Institute West Point.

34. James Pamment, (2020). The EU's Role in Fighting Disinformation: Taking Back the Initiative, Carnegie Endowment for International Peace.

35. Joint Chiefs of Staff, (2014). Joint Publication 3 – 13, Information Operations.

36. Joint Chiefs of Staff, (2018). Joint Publication 3 – 12 Cyberspace Operations.

July 6, 2016, DoD News.

37. Kamya Yadav, (2020). Countering Influence Operations: A Review of Policy Proposals Since 2016, PCIO, Carnegie Endowment for International Peace.

38. Karen Parrish, (2016). CENTCOM Counters ISIL Propaganda

39. Laura Rosenberger and Lindsay Gorman, (2020). How Democracies Can Win the Information Contest, The Elliott School of International Affairs, The Washington Quarterly • 43:2 pp. 75–96.

40. Lt Gen RS Panwar (Retd)(2020) .IW Structures for the Indian Armed Forces

41. Lt Gen RS Panwar (Retd), (2020). Cyber Influence Operations: A Battle Of Wits And Bits-A Call to Action for the Indian Armed Forces, Future Wars(Online).

42. Magnier, M., (2013). Hindu Girl's Complaint Mushrooms into Deadly Indian Riots. Los Angeles Times. Retrieved from http://articles.latimes.com/2013/sep/09/world/la-fg-india-communal-20130910.

43. Mark Galeotti, (2017). Policy Brief: Controlling Chaos: How Russia Manages Its Political War in Europe, London: European Council on Foreign Relations.

44. Martin C Libicki, Strategic Studies Quarterly, (2017). Convergence of Information Warfare

45. Martin C. Libicki, (1995). What Is Information Warfare? , National Defence University.

46. Matthijs A. Veenendaal and Michael, K., (2017). Bots Trending Now: Disinformation and Calculated Manipulation of the Masses. IEEE Technology and Society magazine.

47. Moreau, E., (2017). Internet Trolls and the Many Ways They Try to Ruin Your Day. Lifewire. Retrieved from https://www.lifewire.com/ types-of-internet-trolls-3485894.

48. Nick Fielding & Ian Cobain, (2011). Revealed: US Spy Operation That Manipulates Social Media, The Guardian, 17 March 2011.

49. Noah Tucker and Rano Turaeva, (2016). Public and State Responses to ISIS Messaging: Turkmenistan, CERIA Brief No 15, Central Asia Program

50. Palmertz, B., (2017). Theoretical foundations of influence operations: a review of relevant psychological research. Centre for Asymmetric Threat Studies (CATS), Swedish National Defence College.

51. Pamment, P., Nothhaft, H., Agardh-Twetman, H., Fjällhed, A., (2018). Countering Information Influence Activities: The State of the Art. Lund University: Lund.

52. Pascal Brangetto and MA Veenendaal, (2016).Influence Cyber Operations: The use of cyberattacks in support of Influence Operations, Conference: 2016 - 8th International Conference on Cyber Conflict (CyCon).

53. Paul C., Matthews, M., (2016). The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation: Santa Monica, CA.

54. Pernik, P., (2018). Hacking for influence: Foreign Influence Activities and Cyber-attacks. International Center for Defense and security: Estonia.

55. Peter Pomerantsev and Michael Weiss, (2014). The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money, Institute of Modern Russia.

56. PW Singer and Emerson T Brooking, (2018). Likewar : The Weaponization of Social Media.

57. Renee DiResta et al., The Tactics & Tropes of the Internet Research Agency, New Knowledge, December 17, 2018, https://cdn2.hubspot. net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf; Philip N. Howard et al., The IRA and Political Polarization in the United States, Oxford Internet Institute, August 22, 2018,

58. Renée Diresta, Carly Miller, Vanessa Molter, John Pomfret, And Glenn Tiffert (2020). Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives, Stanford Internet Observatory, Hoover Institution.

59. Richard Stengel (2019). Information Wars – How We Lost the Global Battle against Disinformation & What can We Do About It .

60. Riley.M. , Robertson. J., (2017). Russian Hacks on U.S. Voting System Wider Than Previously Known. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2017-06-13/ russian-breach-of-39-states-threatens-future-u-s-elections

61. Robert S. Mueller, III, “Report On The Investigation Into Russian Interference In The 2016 Presidential Election” (US Department of Justice, Washington, DC, 2019.

62. Ron Schleifer , (2014). Propaganda, PSYOP, and Political Marketing: The Hamas Campaign as a Case in Point, Journal of Political Marketing.

63. Samantha Bradshaw, Hannah Bailey & Philip N. Howard. (2021) Industrialized Disinformation: 2020 Global Inventory of Organised Social Media Manipulation. Working Paper 2021.1. Oxford, UK: Project on Computational Propaganda.

64. Sarah O’Connor with Fergus Hanson, Emilia Currey and Tracy Beattie (2020). Cyber-enabled foreign interference in elections and referendums, Policy Brief

65. SD Pradhan, (2018). Developing Responses to Increasing Challenges of Information Warfare and Influence Operations

66. Sean Cordey, (2019). Cyber Influence Operations: An Overview and Comparative Analysis, Center for Security Studies (CSS), ETH Zurich.

67. Timothy L. Thomas, (2020). Information Weapons: Russia’s Nonnuclear Strategic Weapons of Choice, Cyber Defense Review, Summer 2020.

68. Todd Helmus, (2018). Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe, RAND.

69. U.S. Department of State(2020).Global Engagement Centre (GEC) Special Report : Pillars of Russia’s Disinformation and Propaganda Ecosystem.

70. UK, House of Commons (2020). Intelligence and Security Committee of Parliament Report on Russia.

71. Vosoughi, S., Roy, D., Aral, S., (2018). The spread of true and false news online. Science, pp. 1146 – 1151.

72. Winn Schwartau, (1994). Information Warfare: Chaos on the Electronic Superhighway.