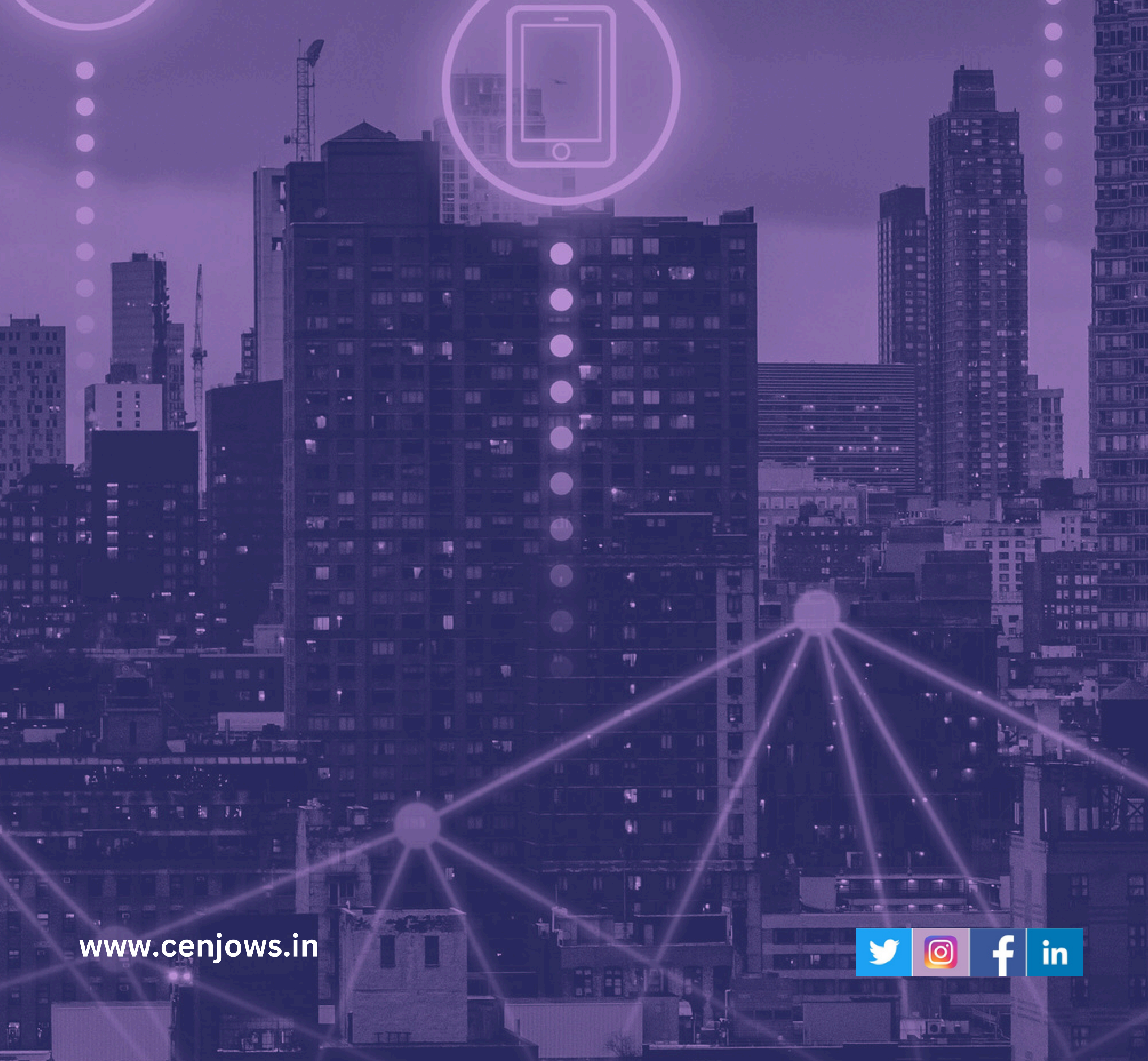
CENJOWS

ISSUE BRIEF
IB/15/24

UNDERSTANDING ROLE OF EMERGING TECHNOLOGY IN CIVIL SOCIETY WARFARE

MR PANKAJ PHANASE



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

UNDERSTANDING ROLE OF EMERGING TECHNOLOGY IN CIVIL SOCIETY WARFARE

Mr Pankaj Phanase is a Research Intern at CENJOWS, New Delhi.

Abstract

Civil Society Warfare (CSW), characterised by the tacit use of non-state actor, is a kind of indirect warfare where confrontation is dispersed in society like blood in capillaries. In the contemporary times, various factors like globalisation, geo-political rivalries, and domestic politics have contributed to its propagation. But the most effective means of its propagation is technological advancement which has nurtured the covert nature of CSW further. Emerging technologies, by their innovative nature as well as incessant factor for societal change, have impacted operation, propagation and threat of CSW. This paper tries to analyse the impact of emerging technologies like digital communications with recent developments like 5G, new trends in surveillance technologies like UAVs, cyber warfare, Artificial Intelligence, Quantum Computing and Blockchain Technologies. The paper has also tried to cover certain factors like transnational network presence, economic inequality, climate change and migration, Election Procedures which are results of technological advancement and are considered as technology induced factors. It has been also attempted to come up with the precise policy suggestions for countering the menace of CSW. By addressing the multifaceted dimensions of this modern warfare, the paper aims to equip India with strategies to protect its social and political fabric from internal and external subversion.

Introduction

Civil society warfare, characterised by conflicts within states involving various non-state actors and external influences, has seen a dramatic increase in recent years. Between 2001 and 2010, approximately five countries annually faced two or more simultaneous conflicts.Currently, around fifteen nations are embroiled in such strife.[1] The proportion of civil wars involving foreign forces has surged twelve-fold since 1991, highlighting the growing internationalisation of these conflicts.[2] This external meddling prolongs wars as foreign actors bear fewer direct costs, thus having less incentive to seek peace. Of all the factors that make modern civil wars so hard to extinguish and so complex, one is the prevalence of corruption and criminality in the conflict zones. The opportunity of power being a short-cut lures many into violence. Climate change acts as an accelerant, although it does not exactly cause them; it does raise the possibility and potential intensity of the conflicts. Additionally, technological developments have assisted all forms of factors to the dangers of civil society warfare domestically as well as cross border interference.

Historical patterns of conflict since 1945 consists of three overlapping waves: the struggle for independence from European colonies, internal power struggles in the newly independent states, and Cold War ideological battles.[3] It has been seen that the number of conflicts and battle deaths decreased after 1991 but soon increased again after 2011.[4] It was in this period that the Arab Spring set conflicts ablaze in the Middle East, when jihadism swept through the Muslim world, and when Russian imperialism under Vladimir Putin raised the stakes of geopolitical conflict. According to David Cunningham of the University of Maryland, the third-party interventions by external powers with their selfish agendas indeed do prolong the civil wars and add on to the casualty count.[5] Because the external actors will less be affected by direct destruction, strong incentives for peace are lacking, hence an entangling of conflicts. But across these heterogeneous complex landscapes, social media venues take centre stage: Facebook, Instagram, and WhatsApp. Banking on enormous user bases with unbelievable reach, their logic and profit driven motive their propagation is morally gloomy.

Every civil unrest disrupts the political environment and the likelihood of broader political disorder increases. External adversaries capitalise on internal divisions, resulting in damage that is indeed more harmful and effective than conventional warfare. Developments in the technology sector that have obliterated traditional forms of conflict, holds the possibility of indirect attacks, which of course, include the information and knowledge sector.

Understanding Civil Society Warfare

Civil Society Warfare or the 4th generation of warfare (4GW), which was often mentioned as a new term of war, is an attack on the character of war. Just as in traditional warfare where state armies fought on ordered battlefields, civil society war plays out the state as an actor waging the war against non-state actors, whether they are terrorist cells or insurgents on its own territory. A novel form of warfare is the disinformation warfare that is mainly used to subvert, divide and manipulate civil society, hence to achieve certain political or military objectives that are often unforeseen.[6]

National Security Adviser (NSA) Ajit Doval has highlighted the critical role of civil society in this form of warfare. He asserts that this kind of warfare focuses more on disturbing the internal fabric of the nation instead of direct military concentration which became complex, costly and sometime even impossible to make into reality. His insights into the issue reveal that actual battlefields have shifted to the societal level, where non-state actors aim to undermine national unity and stability.[7]

The four generations of warfare can be traced as: First-generation warfare was formal battles between state armies, second-generation focused on artillery and firepower, and third-generation brought tactics of speed, surprise, and infiltration to outmanoeuvre enemy forces. Fourth-generation war, however, will see the state losing its monopoly on war, as it is under diffuse, decentralised threats from within the society itself.[8] In civil society warfare, the non-state actor exploits societal cleavages—ethnic, religious, or ideological—to create unrest and rupture the state's grip. It is a warfare of asymmetric nature, with conventional military force responses unable to handle its scope. This places an inordinate burden on internal security forces, like the police, in safeguarding the population against subversion and manipulation. In the contemporary time technology and social media further complicated this kind of civil society warfare. Facebook, WhatsApp, and Instagram can easily be used as channels through which misinformation, violence, and division can be done. Therefore, it becomes easy for non-state actors to fulfil their objectives without much direct confrontation. This places a greater need for comprehensive strategies that involve not only traditional security measures but also the regulation of information flows and societal resilience-building.

Civil society warfare presents a fast-growing and complex challenge in modern states. It calls for manifold efforts to secure the safety of the people from internal dangers and national stability, in an era where the lines separating war from peace, state actors from non-state, and external from internal are increasingly getting blurred. It is necessary to understand emerging technologies impacting the course of civil society warfare in the contemporary era.

1. Technological Factors

1.1 Digital Communications

Digital communication is the most advanced revolution of information production, consumption, and manipulation that changed the way governments, ethnic groups, business organisations function.[9] More specifically, social media platforms, being the most common, are those that allow ordinary people to take part in the communication processes of which leadership is not normally a part and can cause together cross-cultural dialog, yet they also serve as potent tools for political mobilisation. Daniel Abbott, thus, shares the view that Warfare is "a war of information and perception," that is marked primarily by psychological warfare operations, misinformation, and cyberattacks.[10] They function as stages for personalised versions of stories that will be people's emotional trigger points pushing them into action, thus deepening the differences within society. The effectiveness of social media in his political campaigns was proved by Donald Trump's presidential elections in 2017. Trump had already admitted that, “I would not have become President if it had not been for social media.”[11] Similarly, the capability of ISIS, being a virtual entity, to exaggerate its power via Twitter through the use of trends such as #TheAllEyesOnISIS is the reason for many strategic successes.[12]

Social media exploits the illusory truth effect, a powerful tool where repeated claims increase perceptions of truth. It is in this manner that politicians, terrorists, and military organisations use it to plant doubt, division, and distraction in the minds of people, often translating the online clashes into real-life violence. Evan Williams, Founder of Twitter, stated regarding this, “I thought once everybody could speak freely and exchange information and ideas, the world is automatically going to be a better place. But I was wrong.”[13]

1.2 Cyber Warfare

It has been an intrinsic part of this war in civil society and has made a set of paradigm changes in modern conflicts. It is aimed at disrupting, manipulating, and destabilising societal structures without engaging in traditional kinetic activities by using digital technologies.[14] This alternative media space is about becoming "a new battlefield for the mind of people" with the purpose of lessening trust among the public towards the government with the help of counter-narratives.[15] This also links to the broader concept of cognitive war, which refers to targeting human minds to change not only what people think but also how they think and act, thus potentially fractionalizing societies.[16] This hybrid approach blurs the lines between different modes of warfare that traditional forces are incapable of responding to effectively. The opponents may use cyber warfare directed at financial targets to leverage the strategic value of cyber capabilities in undercutting economic stability and institutional trust.[17] The hybrid warfare concept delineates the multi-dimensionality of modern forms of conflicts where cyber warfare is intermeshed with conventional and unconventional techniques, giving rise to complicated threats which are very unpredictable.[18]

Cyber warfare is decentralised in nature, which extends the domains of conflict to physical, information, cognitive, and social spheres. It is this type of expansion that greatly complicates the defence strategies through attacks that are so individually distinctive and dispersed, hence highly difficult to detect and attribute. Cyber warfare manipulates perceptions, thereby changing the context of conflicts, which epitomises the instantiation of strategic objectives without the use of conventional military confrontations.[19] An example to consider is the Hong Kong Protests (2019-2020), in which protesters in Hong Kong used encrypted messaging apps and social media to coordinate activities and share real-time updates while avoiding surveillance. The Chinese government engaged in cyber tactics like hacking and misinformation campaigns in an attempt to discredit the protesting efforts to retain control over the narrative.

1.3 Surveillance

Surveillance is an increasingly important factor in the civil society war, one that dramatically changes the nature of how states behave toward their subjects and conduct internal conflict resolution. Indeed, intensive use of surveillance technologies allows comprehensive monitoring, most often under the screen of national security, while in reality, it is increasingly aimed at suppressing dissent and preventing organised forms of resistance.[20] Indeed, according to Gompert and Gordon, "Counter insurgency deals with political ideologies that may have mass appeal".[21] This shifts the target from individual terrorists to entire populations to be detected on ideological subversion.

India has been a witness to huge investments in surveillance infrastructure, ostensibly for countering terrorism and maintaining public order. But this has deeper implications for civil society. It enhances the capacity of the state to monitor communications and movements and enables it to identify and suppress such threats at their very emergence—the threats to its authority where a legitimate political dissent included. Mass surveillance might be potentially very effective in terms of identifying who may be susceptible to extremism, and therefore preventing the organisation of larger resistance movements.

The use of UAVs in crowd control and monitoring epitomises the integration of surveillance into civil society warfare. The deployment of drones with tear gas to break up crowds shows a definite developing change toward a more pervasive surveillance state.[22] In using emerging technology for surveillance, it not only intimidates but also sets the population in continuous surveillance, creating, through such psychological conditioning, reduced possibilities of organised dissent. Surveillance in this context emerges as a strategic tool in wars of civil society that the modern state deploys to hold on to control and pre-empt opposition. Advanced technologies can be deployed by a modern state to ensure stability at the cost of civil liberties and opening up several other challenges of possible misuse.

1.4 Artificial Intelligence

AI has become a very important element in civil society warfare, in a way that it has made changes to the socio-economic and political sphere. Labor markets being replaced by automation of AI systems have possibility of extremely high unemployment rates which are mainly due to the repetition of such tasks. The lower-income jobs are replaced already, and in the future, we might even see the same thing happening in the fields of medicine, law, and accounting.[23] This technological shift poses the danger of disintegration of the social fabric, aggravation of the socio-economic inequalities, and the destabilisation of the communities that are mostly dependent on the employment sectors which are very vulnerable.

AI, on the other hand, is a medium through which the biases of its human creators are transferred, hence amplifying the already existing socio-economic disparities.[24] The fact that AI development teams are often very homogeneous can lead to the design of algorithms that not only are biased but also reflect and perpetuate the existing prejudices in society instead of being a tool to mitigate global problems.[25] This bias can further marginalise already disadvantaged groups, intensifying social divides and augment unrest. Data and AI tools are more concentrated in a few hands, which brings about significant ethical concerns. If there are no proper governance and ethical systems for AI, then AI's decisions may be biased to the advantage of some interests, there may be privacy violations, and democracy may not be respected. The possible data abuse by powerful entities can lead to manipulation and exploitation, which in turn, can make people lose their trust in institutions and intensify the conflicts in society.[26] AI applications that are malicious possess privacy and security threats which are alarming. The rise of deepfakes, which are almost indistinguishable from real ones, is another factor that harms the public trust and political stability. Deepfakes, for example, can be used to play the game in public opinion, to make the politicians believe in democracy, and to make people act violently.[27] Moreover, AI-based surveillance and hacking tools are also the main causes of the violation of individual rights and national security, which is another factor of society’s destabilisation.

One more functional dysfunction which AI can bring is financial instability, especially by means of algorithmic trading. AI-powered trading systems can act the way unlike people, and can cause financial crises by high-value, high-frequency trades without any human decision making.[28] The unstable states of this kind can lead to the domino effects on the global economy and have a disproportionately high impact on the low-income individuals, while also providing more turbulence in the socio-political relations. The AI′s effect on cognitive and social skills is immense. The over-reliance on AI-based systems might cause the human brains to shrink away from acting and thinking independently, as well as, socialising with others.

1.5 Quantum Computing

Quantum computing is a disruptive technology with dramatic implications for civil society warfare. A quantum computer's astonishing computational power is based on the principles of superposition and entanglement, which are expected to make existing security mechanisms ineffective.[29] This functionality may have far-reaching consequences as it would be able to compromise the security of bank records, military communications, and sensitive government data leading to substantial national and global security risks.[30] The strategic competition between the United States and China is in the light of the significance of quantum technologies (QT). Both the countries see quantum information science as the cornerstone of national security, which leads to the arms race in quantum research and development. The U.S. dominates the field of quantum computing with IBM's 433-qubit Osprey, while China is a Rayleigh winner in quantum communications, holding records such as the Micius satellite and the world′s longest Quantum Key Distribution (QKD) network.[31]

India, sensing the need for a strategic solution, established the National Quantum Mission (NQM) in 2023 and allocated $730 million for quantum research. The projects are meant to create a strong QT system, with the main goal being the development of quantum computing, communication, sensing, and materials. Strategic agencies like DRDO and ISRO are the ones who carry out these projects which reflect the vision of India to strengthen its national security through the use of quantum technologies.[32] With regard to strategic imperatives, it is in 2023 that India launched an investment of $730 million for the promotion of quantum research through the National Quantum Mission. It aims at creating an end-to-end quantum technology ecosystem with prime focus on computing, communication, sensing, and materials. The latter is driven by strategic agencies like DRDO and ISRO, underpinning the fact that India is serious about enriching its potentials in quantum computing to advance its national security.[33]

While quantum computing does come with the potential to break conventional encryptions, it gives an opportunity for absolutely secure, unhackable channels of communication. If it were implemented correctly, this would bring huge gains both in information security and computational powers but would call for very strong countervailing measures against cyber attacks and espionage. With India's NQM, developing a 1000-qubit system and a secure quantum communication network, the country places itself on the pathway to digital infrastructure security and deterrence against foes.[34] Quantum computing can play in the setting of civil society warfare. It will be a threat and an opportunity calling for vigilant strategic investment and international collaboration to harness its potential while mitigating risks

1.6 Blockchain Technology

Blockchain Technology (BT) is a revolutionary factor for reshaping civil resistance and warfare power paradigm. Its centralised structure offers, perhaps, the most censorship-resistant options for impeding activists to bypass government controls and communicate securely, even in oppressive regimes.[35] The technology's decentralised approach of distributing data over a wide network, rather than through centralised ones, is a statement against the conventional power order and allows the less powerful and smaller actors.[36] BT has a key role in the battlefield of the civil society war in the form of a peaceful financing tool. Cryptocurrencies, which are based on a blockchain, make it possible for people to transfer money anonymously, thus facilitating political activities and even illegal actions such as terrorism.[37] The financial dimension makes it quite tough for the authorities to track and control the resources' movement, which is a national security dilemma against the background of the social movements' empowerment.

BT's utility extends into territory well outside that of financial transactions. It enables the creation of decentralised autonomous organisations that can self-organise and sustain without centralised control. In this respect, it is particularly useful for leaderless civil resistance movements based on voluntary participation.[38] Such a possibility of activists joining and supporting causes at very low risk increases their scope and resilience. Blockchain also keeps running communication networks where traditional internet and mobile services are paralysed. Inventions like off-grid Blockchain transactions via radio mesh networks show that this technology is really able to support continuous, secure communication under unfavourable conditions.[39]

Blockchain technology has proved a great influence on civil society in the war as it denies the central power, gives the possibility of anonymous and secure financial transaction, and provides for resilient communication. These capabilities allow for more effective and sustained resistance to authoritative regimes, and thus the dynamics of social and civil conflicts are reshaped.

2. Technology Induced Factors

Innovative technologies are the driving force behind the worsening of the transnational networks, economic disparity, environmental conflict, resource scarcity, and the migration (CSM) nexus, as well as the vulnerability of the election procedures, thereby contributing to CSW. Utilising advanced communication technologies and blockchain enables the creation of transnational networks, which in turn helps to organise and finance not only insurgent groups but also illegal activities. AI, along with automation is the one that grows economic inequality by replacing unskilled workers and this leads to social unrest. Environmental monitoring technologies are a source of information on the breadth of resources, while smart contracts and IoT are the ones that aggravate conflicts over the remaining resources, respectively. The migration nexus is intensified due to the presence of digital platforms that can assist the movement and coordination of displaced populations. Additionally, the elections' vulnerability is enhanced through cyber warfare, where hacking and deepfakes are included, thus, the democratic processes and the trust in governance are undermined. The combined effects of these technologies ensure that societies are unsteady, thus, they are more likely to experience internal conflicts and be subjected to external manipulation.

2.1 Transnational networks

Transnational networks are part and parcel of civil society warfare because they aid in diffusing ideology, resources, and methods across borders, which eventually leads to conflicts and reduced stability at the national level.[40] The emergence of hybrid warfare and international security environment resulted in transnational networks using the platforms provided by globalisation in order to target the domestic fissures and to diffuse false narratives that might cause severe harm to the international image of a country as well as its internal harmony. The phenomenon comes very handy in the case of civil society warfare, wherein most of those actors are non-state and use these networks to their full potential to garner support and resources.

In India, a variety of insurgent movements and social upheavals have been influenced by transnational networks. The insurgency in Kashmir, for instance, has been fed by cross-border support, a potential example of how external networks can sustain and amplify internal conflicts. The Maoist insurgency is an entirely domestic problem, but links with other left-oriented movements across the world prove that there is a transnational dimension of strategy and sustenance networks. These connections provide arms, training, and ideological sustenance, making the conflicts protracted. The role of China and the Western world in these dynamics cannot be discounted. The Chinese Belt and Road Initiative, along with its strategic partnerships in South Asia, actually foreshadows stability in the region. Continuous engagement by China in

Pakistan and other neighbouring countries has created an environment where transnational networks can act more freely and affect civil society warfare through indirect means.[41]

Even more importantly, the Western world, through the use of the internet and social media platforms, has enabled transnational activism.[42] These platforms allow for extremely fast flows of information and mobilisation of support for different causes. These are manipulated by adversaries for media campaigns, insurgencies, and support of sectarianism and regionalism. In this case, the manipulation of ethnic and religious cleavages through transnational networks will go on inflaming societal tensions and thinning the efforts of national integration.[43]

2.2 Economic Inequality

The globalisation has led us to the rising inequality and related disparities and anxieties which have been stoking social discontent and are a major driver of the increased political polarisation and populist nationalism that are so evident today. This link has become potent toll to be used in civil society warfare. This inequality expresses itself at different levels: income disparity, unequal access to resources and opportunities—continuing to foster an environment that is overly prone to conflict. Concentration of wealth in a few hands increases fissures in society and breeds resentment among the subaltern sections of society.[44] Among the populations that feel voiceless and excluded, social unrest is rather a usual result. This flows from the existing social stratification and inevitable exclusion of some groups. The result of this financial inequality and poverty is the possibility of emergence of a powerful ground for the beginning of armed fighting in society. The biggest animosities arise from the distribution of resources that further create divergences between communities. This disposition resulting in the feeling of being abandoned by the authorities is constructive in some states that are not included in economic activities. This inequality is the real problem of the local government and it influences the nation's unity and security in a very negative way. Also, unequal distribution of employment, education, and skill development actually work as a catalyst to civil unrest. Unemployment, combined with the visibility of affluence elsewhere, can lead to frustration and anger, making them susceptible to recruitment by extremist groups or participation in violent protests.[45]

The inequality also leads to deterioration of the quality of governance, leading to skewed policy making in favour of wealthy fostering corruption and crony capitalism.[46]

This undermines public trust in government institutions, escalating widespread dissent and civil disobedience in the society. The most contributing factor to the Maoist crisis, for example, was the result of concentrated land ownership policies in India. Their insurgency is driven by demands for land reform, better wages, and social justice, and thus directly correlates with economic inequalities experienced.[47] In recent times, economic inequality has been fuelled into broad civil unrest, as seen in the case of the Yellow Vest movement of 2018 in France which was triggered by hike fuel tax.[48] However, it has mobilised people over many other broader issues about the high cost of living and economic disparities. Protesters, most of whom were rural and poor, came out against policies that appear to pamper the elite living in cities. The movement reflects the global nature of the issues in India.

2.3 Environmental Conflict, Resource Scarcity, and Migration (CSM) nexus

This interplay of environmental conflict, migration, and resource scarcity understood within the prism of civil society warfare is very important. The “CSM nexus” of climate change, conflict, and migration underlines their interaction: environmental conditions directly affect health and productivity and may spur migration, particularly under conditions of resource scarcity and demographic pressure.[49] For instance, droughts can result in crop failure on a massive scale, resource shortages, and movement of rural people to towns, which pressures the local infrastructure and raises the potential for social tensions to rise, already existing. In fact, empirical studies have revealed that environmental stress leads to conflict through resource scarcity.[50] If resource scarcity is driven by environmental degradation, it will lead to communal conflicts in regions with vulnerabilities. The link, however, is not linear but mediated within the contexts of current socio-political contexts wherein governance is considered as an important mitigating or exacerbating factor of the effects of environmental stressors.[51]

Environmentally induced migration can rise in the potential for conflict in the receiving region. However, these cases were often contingent upon certain conditions, in particular, the existing socio-political landscape and the capacity of local institutions to manage the influx. These interactions are complex, epitomised by the non-linear and spatially divergent aspects of the climate-conflict-migration nexus.[52] While direct impacts of environmental conditions on health and productivity may trigger migration, the social dynamics it sets off are very strongly modulated by the broader socio-economic context. Government policies play a critical role in either mitigating or exacerbating these issues, highlighting the need for informed and adaptive governance to manage the CSM nexus effectively.

2.4 Vulnerability of Election Procedures

The weaknesses of electoral processes have colossal consequences for the happening of civil warfare in the society, which is mostly propelled by the manipulation of electoral systems through various actions: cyberattacks, misinformation campaigns, and legal loopholes.[53] In this respect, erosion of public trust in democratic institutions will lead to increased divisions in society and rising conflict. A very relevant case study, considering this vulnerability, would be that of the 2016 U.S. presidential election, which was marked by a mix of social media manipulation, data analytics, and cyber intrusions that had jointly determined public opinion and the results of elections.[54] With its huge political advertisement and messaging work, Cambridge Analytica had already pointed the way to weaponise data from billions of smartphones as tools of hyper-efficiency for fifth-generation war tactics — a targeted strategy to close feedback loops of misinformation in a furious continuance of polarising the electorate and thus further delegitimising the electoral process.[55]

It has been multiplied by the invention of AI as AI-driven tools can create and distribute deepfakes among other forms of phoney content at incredible speeds, further making this challenge harder for voters in knowing what is truth and invention.[56] What is most worrying, however, is that the attacks usually remain decentralised. Sources remain anonymous, raising risks of missteps and sowing mistrust in defence against intrusion. Geopolitics provides the context where rivalries between the United States, China, and Russia have been waxing hot, which further fuels these vulnerabilities. Each of them has stakes in influencing foreign elections to move the tectonic plates of power in their favour. For example, the allegations of Russian interference in the 2016 US election brought out how state actors might take advantage of electoral vulnerabilities in a bid to further sow discord and attain strategic objectives without having to engage directly on the battlefield.[57]

The electoral system of India has not remained aloof from the same threats. Rising infiltration of social media and digital platforms has opened its elections to the very vulnerabilities. In a way, misinformation and unverified news can spread at an unimaginable speed today. It might go on to influence voter perceptions and hence election outcomes.[58] The integrity of the election procedure is basic to the health of a democracy; any compromise can lead to significant instability and conflict. These vulnerabilities will only be effectively countered through comprehensive strategies operating on technological, legal, and social levels.[59] Among the urgent tasks are improvement of the measure of cybersecurity, transparency of political advertisements, and media literacy of people. Not less important is the international cooperation to establish norms and rules that will help decrease the dangers connected with these sophisticated tactics of election interference.

Policy Recommendations for India to Mitigate the Threat of Civil Society Warfare

A. Enhancing Digital Communications Security

A.1 5G Network Security:

Set the strict rules and the requirements for 5G network deployment. As communication networks are shifting to 5G technology, this has become a vulnerability issue as well. The encrypting of data and the conducting security audits on a regular basis will be the main measures for network protection, as well as cooperation with international cybersecurity agencies in dealing with espionage and hacking.

A.2 Cyber Warfare Preparedness:

Create a comprehensive national strategy for cyber defence. Cyber warfare is a great danger to national security. The implementation of advanced threat detection systems, creation of rapid response teams, and establishment of public-private partnerships will be the factors that will contribute to enhancing cyber resilience. Cybersecurity specialists' training programs and campaigns for the population will also help the country cope with cyber threats.

B. Regulating Surveillance Technologies

B.1 UAV Regulation:

UAVs are for the good when they are used for surveillance and security but can be wrongfully used for malicious purposes. Licensing, geo-fencing, live monitoring, and harsh punishments of illegal use are the measures to be taken for preventing UAVs from posing various risks.

B.2 AI-Powered Surveillance Oversight:

Set up an autonomous supervision unit that will govern the utilization of AI for surveillance. AI-based surveillance can interfere with one's privacy rights if not controlled properly. A separate authority that will control AI surveillance practices will guarantee ethical, transparent, and accountable use of AI, as well as proper balance between security and the fundamental rights of citizens.

C. Promoting Blockchain for Transparency

Integrating blockchain technology with government processes will ensure transparency and prevent corruption. Blockchain can serve as an unalterable record of transactions, hence applicable for voting systems, public procurement, and land registry. Blockchain adoption in these areas will foster transparency, diminish the chances of corruption, and win the public trust in government institutions.

D. Addressing Economic Inequality and Transnational Networks

D.1 Economic Inequality Mitigation:

There is need to aim towards equipping individuals with social and economic skills tailored to fight against income differences which are aggravated by the development of technology. Automation and artificial intelligence can lay off workers with a low salary, consequently widening the gap between rich and poor. Effective measures to implement such as universal basic income, retraining programs, and support for small and medium enterprises can be used to overcome these challenges, ensuring stable and inclusive development.

D.2 Transnational Network Regulation:

Strengthen international cooperation to regulate transnational networks. Transnational networks, often facilitated by technology, can undermine national security. Enhanced international collaboration, information sharing, and joint operations can disrupt illicit networks, including those involved in trafficking, terrorism, and cybercrime.

E. Combating Climate Change and Resource Scarcity

Advocate for the establishment and incorporation of environmentally friendly technologies to fight against global warming and the exhaustion of resources.Climate change can, in fact, make the conflicts and resource scarcity worse. The promotion of renewable energy, intelligent farming, and efficient water management technologies would solve the environmental problems thus preventing resource-based conflicts and ensuring the long-term stability of the region.

F. Securing Election Procedures

Increase the integrity of election procedures through advanced technologies and regulatory measures. Weaknesses in election systems can create crises of democracy and lead to insurgencies. The use of blockchain technology for secure, transparent voting systems, regular audits, and stringent cybersecurity measures will protect the integrity of elections and increase public confidence in democratic institutions.

Conclusion

The threat landscape resulting from civil society warfare is a combination of several factors that call for an approach that is comprehensive and one that recognises the nuances of the situation. In the present times, the clash of technological achievements, global human interaction, and changes in geopolitical realities have drastically turned the nature of conflicts into being more complex and civil societies are therefore more susceptible. For India, the diverse character of its people and its strategic geopolitical location mark the issues of these types. Hence, the key to national stability and security is to deal with the aforementioned problems. Communication and warfare have undergone a sea-change with the advent of technology, leading to new vulnerabilities in cyberspace and social media. The fabrication and proliferation of misinformation and cyber threats highlights the necessity of proper digital literacy and security measures online. In addition, the trend of globalisation has pushed for the formation of transnational interlinked chains and economic disparities, in this way, a cause for the trust among inhabitants and a potential cause for war.

Situation has been such that, for most of the time, India's security has been influenced by what have historically been the geopolitical factors such as the regional skirmishes and power vacuums. The effect of foreign powers on civil wars brings in another dimension to these issues, often leading to continuous occurrences of violence and instability. India has to balance these geopolitical aspects via proactive diplomacy and strategic alliances so as to save its national interests as well as involve in regional peace making. They are some of the big challenges the country has to deal with. For that reason, the preservation of democratic values and the ascertainment of the national unity are surely the countermeasures for these threats. Furthermore, sustainable resource management and the integrity of elections need to be ensured so that the country can bounce back from any such disasters.

Generally, these factors' modulation of each other begets a holistic and strategic approach. India must ascribe to its status, which starts at the ground level of democratic institutions and goes all of the way to its strategic alliances, to endure the threats associated with civil societies affecting the country. India can ensure a stable, secure, and prosperous future, thereby, protecting its national identity and constructing harmony among its diverse population, only if both external and internal threats are dealt with.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Endnotes

[1] Lotta Themner and Peter Wallensteen, "Patterns of major armed conflicts, 2001–10", *SIPRI* https://www.sipri.org/sites/default/files/SIPRIYB1102A.pdf

[2] "In Sudan and beyond, the trend towards global peace has been reversed", *The Economist*, 19 April 2023 https://www.economist.com/leaders/2023/04/19/in-sudan-and-beyond-the-trend-towards-global-peace-has-been-reversed

[3] "In Sudan and beyond, the trend towards global peace has been reversed", *The Economist,* 19 April 2023

[4] Sebastian von Einseidel, "Civil War Trends and the Changing Nature of Armed Conflict", Occasional Power, *United Nations University*, March 2017

https://collections.unu.edu/eserv/UNU:6156/Civil_war_trends_UPDATED.pdf

[5] David Cunningham, “Blocking Resolution: How External States can Prolong Civil War”, *Journal of Peace Research,* March 2010, 115-127, https://cidcm.umd.edu/publicationprofile/1142

[6] Pia Krishnakutty, “Civil society is new frontier of war, can be subverted to harm nation, Ajit Doval says”, *The Print*, 13 November 2021 https://theprint.in/india/civil-society-is-new-frontier-of-war-can-be-subverted-to-harm-nation-ajit-doval-says/765748/

[7] Pia Krishnakutty, “Civil society is new frontier of war, can be subverted to harm nation, Ajit Doval says”, *The Print*, 13 November 2021

[8] “The canon and four generations of warfare”, Australian Army Research Centre, 20 October 2016 https://researchcentre.army.gov.au/library/land-power-forum/canon-and-four-generations-warfare

[9] Yustisia, Ika et al (2023), “The Transformation of Digital Technology: Its Impact on Human Communication”, Future Science

[10] Daniel H. Abbot, The Handbook of Fifth-Generation Warfare (5GW), Nimble Books LLC, 2010

[11] Arooj Sabir, “Social Media and Fifth Generation Warfare”, South Asia Journal, 12 July 2024 https://southasiajournal.net/social-media-and-fifth-generation-warfare/

[12] Audrey Alexander, “DIGITAL DECAY?”, Program on Extremism, *George Washington University*, October 2017 https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/DigitalDecayFinal_0.pdf

[13] Rob Howard, “In 1995, this astronomer predicted the Internet's greatest failure”, *Medium*, 18 July 2017 https://medium.com/the-mission/in-1995-this-astronomer-predicted-the-internets-greatest-failure-68a1c3927e46

[14] Susser, D. & Roessler, B. & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. Internet Policy Review, 8(2). https://doi.org/10.14763/2019.2.1410

[15] Krishnan, A. (2022). Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison. *Journal of Strategic Security*, *15*(4), 14–31. https://www.jstor.org/stable/48707883

[16] Neeraj Mahajan, “COGNITIVE DOMAIN: THE SIXTH DOMAIN OF WARFARE”, Defstrat, Vol 16 Issue 6 Jan – Feb 2023 https://www.defstrat.com/magazine_articles/cognitive-domain-the-sixth-domain-of-warfare/

[17] Frank G Hoffman, “Hybrid Warfare and the Challenges”, Joint Force Quarterly, NDU Press, issue 52, 1st quarter 2009 https://smallwarsjournal.com/documents/jfqhoffman.pdf

[18] VK Ahluwalia, “Hybrid Warfare: Battlegrounds of the Future”, CLAWS Journal, Winter 2019

[19] Robinson, Michael & Jones, Kevin & Janicke, Helge. (2015). Cyber warfare: Issues and challenges. Computers & Security. 49. 70-94. 10.1016/j.cose.2014.11.007.

[20] Ünver, H. A. (2018). *Politics of Digital Surveillance, National Security and Privacy*. Centre for Economics and Foreign Policy Studies. http://www.jstor.org/stable/resrep17009

[21] Gompert, David C., John Gordon IV, War by Other Means -- Building Complete and Balanced Capabilities for Counterinsurgency: RAND Counterinsurgency Study -- Final Report. Santa Monica, CA: RAND Corporation, 2008.

[22] Abhishek De, “Sonic weapons and lubricants: How cops have made farmers' road to Delhi slippery”, India Today, 15 February 2024 https://www.indiatoday.in/india/story/farmers-protest-delhi-haryana-punjab-border-drones-tear-gas-shells-iron-nails-barbed-wires-2502159-2024-02-14

[23] Rebecca Stropoli, “A.I. Is Going to Disrupt the Labor Market. It Doesn′t Have to Destroy It”, Chicago Booth Review, 14 November 2023 https://www.chicagobooth.edu/review/ai-is-going-disrupt-labor-market-it-doesnt-have-destroy-it

[24] Chen Z, “Ethics and discrimination in artificial intelligence-enabled recruitment practices”, Humanities and social sciences communications , 567 (2023). https://doi.org/10.1057/s41599-023-02079-x https://www.nature.com/articles/s41599-023-02079-x#citeas

[25] Shahriar Akter et al, “Algorithmic bias in machine learning-based marketing models”, Journal of Business Research, Volume 144, 2022, Pages 201-216, ISSN 0148-2963, https://doi.org/10.1016/j.jbusres.2022.01.083. https://www.sciencedirect.com/science/article/pii/S0148296322000959

[26] Janna Anderson and Lee Rainie, “Themes: The most harmful or menacing changes in digital life that are likely by 2035”, Pew Research Centre, 21June 2023 https://www.pewresearch.org/internet/2023/06/21/themes-the-most-harmful-or-menacing-changes-in-digital-life-that-are-likely-by-2035/

[27] “Deepfakes can help sway public opinion, discredit people or politicians: Experts”, The Ecomonic Times, 11 March 2024 https://government.economictimes.indiatimes.com/news/secure-india/deepfakes-can-help-sway-public-opinion-discredit-people-or-politicians-experts/108386133

[28] Jessica Power, “AI Trading: How AI Is Used in Stock Trading”, Built In, 6 May 2024 https://builtin.com/artificial-intelligence/ai-trading-stock-market-tech

[29] Michael Tabb et al, “How Does a Quantum Computer Work?”, Scientific American, 7 July 2021, https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/

[30] Ondrej Burkacky, “What is quantum computing?”, Mckinsey and Company, 5 April 2024 https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

[31] Jane Lee, “IBM launches its most powerful quantum computer with 433 qubits”, 9 November 2022 https://www.reuters.com/technology/ibm-launches-its-most-powerful-quantum-computer-with-433-qubits-2022-11-09/

[32] Matt Swayne, “India Announces $730 Million-Plus National Quantum Mission”, The Quantum Insider, 20 April 2023, https://thequantuminsider.com/2023/04/20/india-announces-730-million-plus-national-quantum-mission/

[33] Ankit Tiwari, “The Security Implications of Quantum Computing and India′s National Quantum Mission”, The Diplomat, 9 June 2023 https://thediplomat.com/2023/06/the-security-implications-of-quantum-computing-and-indias-national-quantum-mission/

[34] Ankit Tiwari, “The Security Implications of Quantum Computing and India′s National Quantum Mission”

[35] Sfetcu, Nicolae. (2024). The Revolutionary Role of Blockchain Technology in Communication. IT & C. 3. 10.58679/it88509.

[36] Armin Krishnan, "Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations", Journal of Strategic Security, Vol. 13, No. 1 (2020), pp. 41-58 https://www.jstor.org/stable/10.2307/26907412

[37] Anshu Siripurapu *and* Noah Berman, "The Crypto Question: Bitcoin, Digital Dollars, and the Future of Money", Council on Foreign Relations, 17 January 2024 https://www.cfr.org/backgrounder/crypto-question-bitcoin-digital-dollars-and-future-money#:~:text=Blockchains do not record real,their transactions can be traced.

[38] Singh, Madhusudan & Kim, Shiho. (2019). Blockchain technology for decentralized autonomous organizations. 10.1016/bs.adcom.2019.06.001.

[39] Armin Krishnan, "Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations"

[40] Ann Florini, "Transnational Civil Society Networks", Carnegie Endowment, 14 March 2000 https://carnegieendowment.org/events/2000/03/transnational-civil-society-networks?lang=en

[41] Muhammad Ashraf Nadeem, "Fifth Generation Warfare and its Challenges to Pakistan", Pak. Journal of Int′L Affairs, Vol 4, Issue 1 (2021)

[42] Mark Kirsten, "Has Social Media Successfully Reinvented Social Activism?", Justice in Conflict, 2 June 2012 https://justiceinconflict.org/2012/06/02/has-social-media-reinvented-social-activism-a-debate/

[43] Jules Baleyte et al, "Social Inequalities and the Politicization of Ethnic Cleavages in Botswana, Ghana, Nigeria, and Senegal, 1999-2019", *World Inequality Lab*, September 2020 https://wid.world/document/social-inequalities-and-the-politicization-of-ethnic-cleavages-in-botswana-ghana-nigeria-and-senegal-1999-2019-world-inequality-lab-wp-2020-18/

[44] Helena Vieira, "The long-run tendency for wealth to concentrate in a few hands", *LSE blog*, 27 April 2017 https://blogs.lse.ac.uk/businessreview/2017/04/27/the-long-run-tendency-for-wealth-to-concentrate-in-a-few-hands/

[45] Polacko, M. (2021). Causes and Consequences of Income Inequality – An Overview. *Statistics, Politics and Policy*, *12*(2), 341-357. https://doi.org/10.1515/spp-2021-0017

[46] Rose-Ackerman, Susan. (2004), "The Challenge of Poor Governance and Corruption", *Revista Direitogv*. 1.

[47] Behera, A. (2019), "Politics of Good Governance and Development in Maoist Affected Scheduled Areas in India: A Critical Engagement", *Studies in Indian Politics,* 7(1), 44-55. https://doi.org/10.1177/2321023019838649

[48] "France′s yellow vest movement has morphed far beyond a carbon tax protest, Stanford economist says", *Stanford Report*, 23 January 2019 https://news.stanford.edu/stories/2019/01/know-frances-yellow-vest-movement

[49] Abel, G., Brottrager, M., Crespo Cuaresma, J. & Muttarak, R. (2019) "Climate, conflict and forced migration." *Global Environmental Change*, 54, 239–249.

[50] Homer-Dixon, T. F. (1994), "Environmental Scarcities and Violent Conflict: Evidence from Cases", *International Security*, *19*(1), 5–40. https://doi.org/10.2307/2539147

[51] Abel, G., Brottrager, M., Crespo Cuaresma, J. & Muttarak, R. (2019) “Climate, conflict and forced migration.”

[52] Homer-Dixon, T. F. (1994), “Environmental Scarcities and Violent Conflict: Evidence from Cases”

[53] Gretchen Bueermann and Daniel Dobrygowski, “From deepfakes to social engineering, here's what to know about elections, cybersecurity and AI”, Centre for the Fourth Industrial Revolution, World Economic Forum, 8 November 2023
https://www.weforum.org/agenda/2023/11/elections-cybersecurity-ai-deep-fakes-social-engineering/

[54] Allcott, Hunt & Gentzkow, Matthew (2017), “Social Media and Fake News in the 2016 Election”, *Journal of Economic Perspectives,* 31. 211-236.

[55] Harshil Kanakia, Giridhar Shenoy, Jimit Shah (2019), “Cambridge Analytica - A Case Study”, Indian Journal of Science and Technology, ISSN: 0974-6846, Vol: 12, Issue: 29, Page: 1-5

[56] “How AI-powered tools, deepfakes pose a misinformation challenge for Internet users”, *The Economic Times,* 19 March 2023
https://economictimes.indiatimes.com/news/how-to/how-ai-powered-tools-deepfakes-pose-a-misinformation-challenge-for-internet-users/articleshow/98770592.cms?from=mdr

[57] “Report on the Investigation into Russian Interference in the 2016 Presidential Elections”, Volume 1, *US department of Justice*, March 2019
https://www.justice.gov/archives/sco/file/1373816/dl

[58] Samriddhi Sakunia, “AI and Deepfakes Played a Big Role in India′s Elections”, Mew Lines Magazine, 12 July 2024
https://newlinesmag.com/spotlight/ai-and-deepfakes-played-a-big-role-in-indias-elections/

[59] Ben Feringa and Sir Paul Nurse, “Facts over fiction: Why we must protect evidence-based knowledge if we value democracy”, *World Economic Forum*, 16 January 2024
https://www.weforum.org/agenda/2024/01/protect-evidence-based-knowledge-democracy-misinformation/