Strategic Digital Information Operations

IHSAN YILMAZ
SHAHRAM AKBARZADEH
GALIB BASHIROV

SEPTEMBER 10, 2023
DOI.ORG/10.55271/PP0024A
BIOS

IHSAN YILMAZ is Research Professor and Chair of Islamic Studies and Inter-cultural Dialogue at the Alfred Deakin Institute for Citizenship and Globalisation (ADI), Deakin University, Melbourne, Australia. He has conducted research on nation-building; citizenship; ethnic-religious-political identities and their securitization (Middle East, Pakistan, Indonesia); minority-majority relations (Australia, Turkey, the UK, and the USA); socio-legal affairs, identities, belonging and political participation of Muslim minorities in the West (the UK, Australia, and the USA); Islam-state-society relations in the majority and minority contexts; global Islamic movements; political Islam in a comparative perspective; Turkish politics; authoritarianisation; Turkish diasporas (the UK, Australia, the USA); transnationalism; intergroup contact (Australia); and politics of victimhood (Australia, Turkey).

Dr SHAHRAM AKBARZADEH is Convenor of Middle East Studies Forum (MESF) and Deputy Director (International) of the Alfred Deakin Institute for Citizenship and Globalisation, Deakin University (Australia). He held a prestigious ARC Future Fellowship (2013-2016) on the Role of Islam in Iran's Foreign Policy-making and recently completed a Qatar Foundation project on Sectarianism in the Middle East. Prof Akbarzadeh has an extensive publication record and has contributed to the public debate on the political processes in the Middle East, regional rivalry and Islamic militancy. In 2022 he joined Middle East Council on Global Affairs as a Non-resident Senior Fellow. Google Scholar

Dr GALIB BASHIROV BASHIROV is an associate research fellow at Alfred Deakin Institute for Citizenship and Globalization, Deakin University, Australia. His research examines state-society relations in the Muslim world and US foreign policy in the Middle East and Central Asia. His previous works have been published in Review of International Political Economy, Democratization, and Third World Quarterly.

Funding: This research was funded by Gerda Henkel Foundation, AZ 01/TG/21, Emerging Digital Technologies and the Future of Democracy in the Muslim World.
In this paper, we introduce the concept of “Strategic Digital Information Operations” (SDIOs), discuss the tactics and practices of the SDIOs, explain the main political goals of state and non-state actors in engaging with SDIOs at home and abroad, and suggest avenues for new research. We argue that the concept of the SDIOs presents a useful framework to discuss all forms of digital manipulation at both domestic and international levels organized by either state or non-state actors. While the literature has examined the military-political impacts of the SDIOs, we still don’t know much about societal issues that the SDIOs influence such as emotive political mobilization, intergroup relations, social cohesion, trust, and emotional resonance among target audiences.
INTRODUCTION

In recent years, the convergence of the digital realm and political sphere has created a dynamic environment where a wide range of state and non-state actors try to leverage digital platforms to pursue their political goals. This trend includes diverse cases, spanning from the continual targeting of autonomous media establishments in nations like Egypt and Turkey to the deliberate manipulation of electoral processes in democratic countries such as the United States (US) and the United Kingdom (UK), while also extending its reach to include extremist groups such as ISIS who use digital platforms for their propaganda endeavours (see Ingram, 2015; Theohary, 2011). These “Strategic Digital Information Operations (SDIOs),” as we call them here, refer to efforts by state and non-state actors to manipulate public opinion as well as individual and collective emotions by using digital technologies to change how people relate and respond to events in the world. As such, SDIOs involve deliberate alteration of the information environment by social and political actors to serve their interests.

We use this term – SDIOs – because it combines several facets of digital manipulation at both national and international levels. “Information Operations” is a term social media companies like Facebook have adopted to describe organized communicative activities that attempt to circulate problematically inaccurate or deceptive information on their platforms. These activities are strategic because rather than being purely communicative, they are driven by the political objectives of state and non-state actors (see Starbird et al., 2019; Hatch, 2019). We add the concept ‘digital’ to emphasize the distinction between the old ways of information operations and the new ones that operate almost specifically in the digital realm and use much more sophisticated tools such as artificial intelligence (AI), machine learning, and algorithmic models to disseminate information. Of course, some aspects of digital information operations have been carried over from the non-digital environments that have been mastered over the past century. Nonetheless, the affordances of the digital environment have provided not only radically new and sophisticated tools but also an opportunity for much wider dissemination and reach for strategic information operations.

The SDIOs involve various tactics used by political groups who try to shape the online environment in their favour. Their goal is to control the flow of information, where politics and social actions meet. We note that these tactics can cross borders between countries: these operations don’t just target people within a country; they also aim to reach people in other nations. In this article, we briefly discuss the tactics and practices of the SDIOs, explain the main political goals of state and non-state actors in engaging with SDIOs at home and abroad, and present venues for new research.
Tactics and Practices of

As researchers started to examine the many ways in which state actors have tried to manipulate domestic and foreign public opinion in their favour, disinformation has become the main focus of their analysis with an emphasis on spreading fake news, conspiracy theories, and outright lies. Various forms of disinformation have been used in order to create doubt and confusion among the consumers of malign content. Spreading conspiracy theories makes people doubt the truth, which weakens trust in social and political institutions. Moreover, sharing fake news or other fabricated stories weaves a web of lies that shapes what people think. While the latter has certainly been effective in manipulating public opinion, observers have noted recently a shift in emphasis from disinformation to more sophisticated and less discernable means of manipulation.

The aforementioned shift has taken place due to the growing awareness of the fake news and lies in digital environments on the part of both users and digital platforms. As platforms such as Twitter and Facebook have increased their clampdown on such content and as users have become more capable in spotting them, state and non-state actors have moved to more sophisticated means of digital manipulation where content is carefully designed to change how people see things. For example, instead of outright lies or fake news, strategic actors have started to spread half-truths that create a specific version of events by conveying only part of the truth (Iwuoha, 2021). Moreover, these actors have made massive investments on smart public relations messages and clever advertisements to prop up their messages. An important tactical goal has become not simply to deceive the audience but more so to 'flood' the information space with not just false, but also distracting, irrelevant, and even worthless pieces of information with the help of trolls and bots, hired social media consultants and influencers, as well as genuine followers and believers (Mir et al., 2022).

For example, observers noted how a prominent strategy of the Chinese domestic propaganda is to 'drown out' dissident voices through incessant propagation of the government messaging, a campaign called ‘positive energy’ (Chen et al., 2021). The Orwellian campaign involved not only the use of a massive influencer and troll army to promote government messaging but also the forceful testimony of the Uyghur people. In one instance for example, seven people of Uighur descent were brought to a press conference to share their stories of “positive energy” and made-up hype against China to disprove allegations of mistreatment by the Chinese government (Mason, 2022). As such, SDIOs encompass all these tactics and practices rather than merely focusing on means of disinformation that have so far dominated the research into digital manipulation. It also shows the ability of SDIOs to adapt and change over time based on the operational context. While disinformation through direct messages remains a consistent approach, actors
increasingly move towards using subtler tactics to create distractions and cause confusion among their audience, which weakens the basis of well-informed political discussions. For example, the Egyptian government has flooded the information space with the news of the ‘electricity surplus’ and the future of Egypt as ‘an electricity carrier for Europe’ amidst an ongoing economic crisis in the country that has left millions of Egyptians without access to reliable electricity (Dawoud, 2023).

At the heart of discussions about strategic digital information operations lies the creation of narratives carefully designed to connect with their intended audiences. These narratives aren’t random; instead, they’re tailored to match how the recipients think. The interaction between these narratives and their audiences involves psychology, culture, and emotions. How the audience reacts depends not only on how convincing the content is, but also on their existing beliefs, biases, and cultural contexts (Bakir and McStay, 2018). While some people might approach these narratives with doubt, others could be drawn into self-reinforcing cycles, giving in to confirmation bias and manipulation. This back-and-forth underlines the close link between creators and consumers of strategic narratives in the digital era.

Among the many narrative tropes that SDIOs use, we want to note the increasing role ascribed to historical and religious notions to influence public opinion and political discussions. SDIOs mix past grievances and religious beliefs to make their stories more impactful and believable. Bringing up old injustices can stir up strong patriotic feelings or strengthen shared memories. At the same time, using religious stories can tap into deeply held beliefs, making people think there is divine approval or a connection to common values. This blend of history and religion makes their stories powerful and emotional, making them more effective. In Turkey, for example, the state authorities have disseminated victimhood narratives that largely rested on conspiracy theories and half-truths in order to legitimize their rule and quash dissent (Yilmaz and Shipoli, 2022). Research has noted that Islamic religious ideas and the reconstructed history of the Ottoman collapse have been strategically inserted into such narratives to elevate their influence among the Turkish masses (Yilmaz and Albayrak, 2021; Yilmaz and Demir, 2023).

Finally, it's important to stress that these information operations aren't always coordinated by automated bots or pre-planned campaigns. Sometimes, they happen naturally through implicit coordination among various participants, which makes the situation even more complex. Starbird et al.'s (2020) research demonstrates that online information operations involve active participation by human actors. The messages these operations spread are disseminated by utilizing online communities and various sources of information. As such SDIOs can be ‘cooperative’ endeavours in that they...
do not always rely on mere “bots” and “trolls,” but also encompass the contribution of online crowds (both knowingly and unknowingly) in the propagation of false information and political propaganda. For example, during the Russian information operations in the wake of the 2016 US Presidential elections, agents of the Internet Research Agency (RU-IRA) based in St. Petersburg worked together through the operation of more than 3,000 accounts that presented themselves as people and organizations belonging to the American political spectrum (such as the Black Lives Matter and the Patriotic Journalist Network). While undertaking such ‘orchestrated’ activity, the RU-IRA also managed to integrate organic communities by impersonating activists within those online communities, building networks within those communities, and even directly contacting ‘real’ activists. In some cases, RU-IRA agents directly collaborated with activists to organize physical protests in the US (see Walker, 2017).
Goals of SDIOs

SDIOs span both national and international contexts, targeting domestic and foreign audiences through an array of tactics to achieve the political goals of their organizers. Looking at the domestic realm, SDIOs have influenced the functioning of the government and social and political institutions. In many instances, authoritarian governments use digital platforms to influence individuals’ opinions through stories, emotions, and viewpoints that are carefully designed to resonate with specific groups of the population. Their toolkit includes a range of elements, such as conspiracy theories that legitimize a government policy or deflect attention from a government failure, or that create doubt on the arguments of the opposition parties and social actors. Governments may also present narratives where they portray themselves as victims, manipulate facts, and spread distorted statements. For example, in Egypt, the government’s digital narratives have portrayed independent media outlets as agents of Western conspiracies designed to infiltrate and destroy the Egyptian social and political fabric. Similarly, the civilian presidential candidates against President Sisi have been labelled Western puppets created to destabilize Egypt (Michaelson, 2018). In China, the CCP government has used media management platforms such as iiMedia to control public opinion, including providing early warnings for ‘negative' public opinions and helping guide the promotion of ‘positive energy’ online (Laskai, 2019).

It must also be noted that these narratives, particularly those that employ victimhood tropes, are strategically employed to trigger
various emotions among the masses. In Turkey, for example, the Erdogan regime has consistently abused a victimhood claim that rested mainly on the already-existing emotions of the masses such as envy, disgust, humiliation, hatred, anxiety, and anger (Yilmaz, 2021). These emotions are triggered and aroused by government elites as well as government-controlled media in order to legitimize the Erdogan regime’s authoritarian rule and deflect attention from its failures (see Yilmaz, 2021; Tokdogan, 2019).

While both sets of actors pursue political goals through digital manipulation, there are certain differences between state and non-state actors when it comes to utilizing the SDIOs. On the one hand, the state actors tend to be well-resourced and possess good infrastructure of human and technological capital. They tend to have access to a range of digital tools to be used in domestic and foreign contexts, whether to silence the critics and legitimize their rule at home or destabilize their adversaries and extend their geopolitical influence abroad. They tend to carefully plan campaigns to infiltrate foreign information systems, reshape stories, and generate social conflicts, all of which take long-term thinking and strategic foresight. On the other hand, non-state actors, including hacktivist groups and extremist organizations, may lack resources but they tend to be more adaptable to new environments. They use digital platforms to promote their causes, attract supporters, and amplify their voices. These players manoeuvre through the digital world with agility, reflecting the changing nature of the medium.

**A Specific, International SDIO: Sharp Power**

SDIOs undergo a transformation into tools of geopolitical orchestration and influence projection. In this context, digital strategies manifest as instruments designed to strike a chord with international audiences. They sow seeds of social and political division in target countries that perpetrators try to destabilize. These efforts generate support for
both domestic and foreign policy objectives of the perpetrators, often exceeding the boundaries of the conventional notion of soft power and giving rise to what is termed “sharp power” (Walker, 2018). This variant of influence extends beyond the benign strategies commonly associated with “soft power,” taking on a more coercive character where “it seeks to pierce, penetrate, or perforate the political and information environment” (Walker, 2018: 12; Fisher, 2020; Elshaw and Alimardani, 2021).

The emergence of “sharp power” has denoted a significant shift in the dynamics of external influence, as digital platforms are being used to coercively reshape geopolitical interactions between major powers such as the US, China, and Russia, as well as middle powers such as Australia, Turkey, and Egypt. For example, over the last decade, Australia, its public authorities, media entities, and civil society organizations have been systematically targeted by Chinese sharp power operations that included lavish donations to campaigns of useful political candidates, harassment of journalists, and spying on Chinese students in university campuses (The Economist, 2017).

**Social Impacts of SDIOs**

The study of strategic information operations is not new as scholars noted the US and Soviet attempts at influencing each other’s information environment since the start of the Cold War (see Martin, 1982). Nonetheless, we note that the strategic information operations have been used mostly in two fields of study: military influence and social media analysis, with the political science literature mostly discussing the elements of the concept without fully operationalizing it.

On the one hand, scholars working within military studies have rightly pointed out the strategic reasoning of information operations for international politics (see Rattray, 2001; Kania and Costello, 2018). For example, Kania and Costello (2018: 105) showed how the creation of the Strategic Support Force within the Chinese army structure was aimed at “dominance in space, cyberspace, and the electromagnetic domain,” thus generating synergy among these three domains, and building capacity for strategic information operations. States have also been manipulating the information environment to influence the internal affairs of their adversaries for decades. This has led to discussion of information operations as a potential threat to national security and stability (Hatch, 2019).

On the other hand, those working on social media analysis have tried to explain how these information operations have been carried out in social media environments. Researchers have identified technical means through which sophisticated tools of manipulation have been put in place in platforms such as Twitter and Facebook that led to the spread of dis/misinformation (see Starbird et al., 2019). Among other things, this literature has also helped us to understand why certain pieces of information resonate with users and generate a response (such as those that are more surreal, exaggerated,
impressive, emotional, persuasive, clickbait, and shocking images tend to generate better results).

The political science literature has noted various ways in which specific forms of mis/disinformation have affected political discussions in mostly democratic countries without utilizing the SDIOs as an umbrella term. In democratic contexts, the rapid dissemination of misinformation and divisive narratives poses a substantial threat, corroding informed decision-making and hindering the robust exchange of ideas. Trust, a cornerstone of functional democracies, becomes fragile as manipulation proliferates, eroding institutional credibility and undermining the fundamental tenets of democratic governance. For example, in the US, the Russian information operations around the 2016 Presidential Elections targeted key political institutions such as the political parties, the Congress, and the Constitutional Court through hacking, manipulative messaging, and social media campaigns, leading to erosion of trust among American citizens on these institutions (see Benkler et al., 2018).

While the literature covered such issues, we note that social aspects have not received as much discussion so far. We have seen that the SDIOs create significant social impact in terms of social cohesion, polarization, intergroup relations, and radicalization just to name a few. However, the literature's discussion of these concepts has been limited to technical or political aspects. For example, when the literature examines polarization, they either try to demonstrate how these operations polarize the discourse on the internet, or they focus on political polarization (e.g., between the left and the right, or the majority and the minorities) (e.g., Howard et al., 2018; Neyazi, 2020) while overlooking the wider societal polarization and corruption. Moreover, we need further investigations into how social media platforms amplify the impact of information operations on group dynamics, specifically, whether the content on social media exacerbates polarization and reinforces group identities. This is premised on the fact that the impact of SDIOs extends beyond individual psychology, permeating the collective fabric of societies and democratic institutions. By exploiting digital platforms, these operations can foster polarization, exacerbate existing divisions, and undermine the foundations of social cohesion.
Impacts of SDIOs on Individual and Collective Emotions

In the context of social issues, an important underexplored aspect is the emotional dimension. The SDIOs aim to provoke a wide range of emotions among their targets, including negative, positive, and ambivalent feelings. They aim to generate these emotional responses to achieve various political goals such as gaining support for their political causes, undermining opposing groups, eroding trust in society, marginalizing minority groups, and making people question the credibility of independent media outlets. These operations are usually planned to trigger specific emotional reactions that align with the intentions of the perpetrators. For example, Ghanem et al. (2020) found that the propagation of fake news in social media aims to manipulate the feelings of readers “by using extreme positive and negative emotions, triggering a sense of ‘calmness’ to confuse the readers and enforce a feeling of confidence.” However, we need further research to understand how such emotional responses generate social impacts such as intergroup resentment, xenophobic fear, and anger, potentially leading to societal dissent and upheaval. Conversely, positive emotions like empathy and camaraderie can foster social unity and rally support around social causes. Therefore, the strategic coordination of emotional experiences stands as an important dimension of SDIOs that needs further research.

The final underexplored area we want to emphasize pertains to the content of strategic narratives, including the social and political reasons behind their
resonance within target societies. For example, in addition to the content of conspiracy narratives, new research needs to identify why and how certain narratives work in specific social contexts and not in others. Research needs to investigate how historical events, cultural norms, and collective memories shape the reception and resonance of strategic narratives. For instance, narratives that invoke historical grievances might gain traction in societies with unresolved historical conflicts. Further research can explore how strategic narratives tap into individuals’ sense of identity and belonging. Narratives that align with or reinforce a group’s identity can gain more resonance, as they validate existing beliefs and foster a sense of unity.
In this paper, we introduced the concept of the Strategic Digital Information Operations (SDIOs), discussed the tactics and practices of the SDIOs, explained the main political goals of state and non-state actors in engaging with SDIOs at home and abroad, and presented avenues for new research. We highlighted that the concept of the SDIOs presents a useful framework to discuss all forms of digital manipulation at both domestic and international levels organized by either state or non-state actors. We noted that while the literature has examined military-political impacts of the SDIOs, we still don’t know much about societal issues that the SDIOs influence such as intergroup relations, social cohesion, trust, and emotional resonance among target audiences.

Understanding how audiences perceive and react forms the foundation for generating effective countermeasures against the harmful impacts of SDIOs. Initiatives aimed at promoting digital literacy, critical thinking, and the ability to discern media authenticity will empower individuals to navigate the potentially deceptive terrain of manipulated information. Additionally, creating transparency and accountability in algorithms that digital platforms use and rely on, along with dedicated fact-checking initiatives, will enhance the tools necessary to distinguish between truth and deceit. Furthermore, collaborative efforts involving governments, technology companies, and civil society entities can serve as a strong defense against the corrosive effects of manipulation, safeguarding the integrity of democratic discourse and the informed participation of citizens.

Finally, we note that the examination of SDIOs demands a comprehensive range of methodologies that arise from various disciplines including, quantitative and qualitative analysis that aims at revealing patterns of engagement and shifts in emotions, tracing the pathways of information dissemination, and mapping the networks of influence. Ethnographic investigations that delve into the personal experiences of participants can provide a human-centred perspective, showing the psychological, emotional, and cognitive dimensions of manipulation. Effective collaboration among technology experts, academic scholars, and policymakers can foster a deeper understanding of digital operations work and generate influence.
REFERENCES


