Influence Operations: Challenging the Social Media – Democracy Nexus

Ignas Kalpokas

Social media has traditionally been unequivocally seen as facilitating democratic transitions and challenging the power of autocratic regimes. Some most recent research, however, contradicts this established narrative, and as a result, this article first aims to show that social media does not have intrinsic political qualities of its own. Rather, they are contingent upon the offline conditions and the actors who use social media. Then, building on the contingent nature of this media, the author aims to show how social cyberspace enables a new kind of influence operations that can be carried out instantly, globally, and with the help of the victims themselves (referred to as ‘sofa warriors’). Finally, the conflict in Ukraine is presented as an example of how social media influence campaigns can be employed in hybrid warfare.
Traditionally, the internet and social media (SM) have been seen as game changers in democratic struggles, enabling activists and promoting freedom. And yet, as will be shown, there are also mounting evidence challenging the social media-democracy nexus. This article aims to take one step further by arguing that not only SM does not have any essence of its own but also it can be used for influence operations by hostile foreign actors. This proposition is then demonstrated in the context of hybrid war and the conflict in Ukraine.

As the popular narrative has it, “[t]oday, anyone with an internet connection and a Twitter account can make the news. If you choose, the powers that be are you.”¹ Indeed, the advent of “citizen journalism,” through a combination of SM and devices capable of capturing images and keeping individuals constantly connected, has significantly democratised the information landscape. Still, it is doubtful whether the optimism is completely deserved since it is equally true that, in military-strategic terms, “new media [is] a significant enabler of ‘that element of combat power called information.’”² The fact that the British Army has recently decided to create a new brigade tasked with performing information operations³ is another proof of that point. And yet, commendable as this addition to military force might be, there is a need to take one step further by dissociating influence operations from conventional military ones in terms of both offence and defence. In this respect, the recent addition to the European Union agenda of protection against information influence, understood as a continuous process,⁴ seems to be a step in the right direction.

Notably, a significant part of the pro-democracy social media literature, including that used in this article, draws on the Arab Spring (it is, undoubtedly, the most widely discussed case study), whereas the contrary potential is mainly illustrated through the conflict in Ukraine. These two crises are very different: one represents popular uprisings dealing with political reform, the other refers to two governments (and their proxies) clashing over control of a specific territory. However, that is precisely the point, emphasising radically different uses and context dependence of social media.

Social Movements and Social Media: Contradiction and Contingency

Initially, the positive side of SM has to be outlined. Certainly, SM has had significant impact in enabling pro-democracy movements and facilitating expression of civic discontent. Although what follows is not an exhaustive account of SM’s positive contribution, the main changes are nevertheless covered. And yet, as it is argued later, these same contributions can easi-
ly be inverted and used to strengthen authoritarianism and/or embark on influence operations.

First of all, SM is a valuable addition to social movements’ toolkit. Generally, the crucial role of SM in spreading information, mobilising people, creating protest networks both nationally and internationally is emphasised. By erasing distance, it is argued, SM succeed in “making the remote local,” i.e. enabling people to connect across geographical distances. Clearly, SM has the potential to facilitate “multiple and diverse network spheres” that, if translated to offline action (which is by no means unproblematic), can encourage democratic tendencies. Crucially, citizens are no longer forced to passively consume information but are, instead, empowered to challenge centrally sourced news and put forward their own perspectives avoiding official networks. As a result, SM plays a vital part in disseminating otherwise unavailable information and facilitating its exchange. In this way, SM is seen to offer “more readily available, immediate and equal access to public sphere.” It appears that, for example during the Arab Spring, SM did enable “direct and relatively constant channels of communication and diffusion of ideas,” sustenance of collective action, and global transmission of information.

Next, it is quite likely that SM affects users’ choices and actions. SM may play a role in empowerment and mobilisation, as research shows that SM users are more likely to protest and be otherwise politically engaged, also being more active and better informed than non-users. It has even been argued that SM fosters an ethic of “perpetual participation.” Organisation of such protests themselves might be affected as well since movements enabled by SM tend to operate under a “logic of aggregation,” whence viral flow of information acts as an impetus for aggregation of people in offline spaces. Even SM discussions originally intended for criticism only can evolve into offline protests. As such, SM might be seen as enabling latent opposition to take material forms and creating drive for regime change or challenges to the global order seemingly out of nowhere.

Among other notable claims, it is even suggested that internet penetration, supported by adequate hardware and broadband, by itself “facilitates democratic change by cultivating pro-democratic attitudes.” Moreover, a Tunisian case study appears to show that SM can also make a positive contribution to post-regime change development. In short, it is relatively easy to see SM, and internet more generally as “liberation technology.” Nevertheless, the record is contradictory. Wid-
er research also shows that SM is equally capable of spreading anti-democratic ideas that are sometimes even more hard-line than the regime itself, and anti-democratic participation via SM is not unheard of. This observation, then, leads to the other side of SM – one that acts as facilitator of authoritarian regimes.

Indeed, there is an emerging strand of research that challenges the determinism of SM almost unavoidably leading to democratisation. In fact, depending on the actual political culture of a particular authoritarian regime, SM might not be widely used to challenge it, and home-grown Social Networks in particular seem to be relatively passive and are easily controlled by the government. Even more importantly, many authoritarian governments have learnt to co-opt SM, using it to 1) gather information about grievances, 2) keep local officials in check through public opinion, 3) shape public discourse thus boosting legitimacy, and 4) mobilise and coordinate their support base. Moreover, since no regime can function without at least some public support, SM can be used to mobilise those supporting the status quo. All these uses significantly draw on the supposedly empowering SM contributions outlined above. Also, autocratic regimes use SM to discredit the opposition and shape the discourse of their support base. Those supportive groups are not only comprised of people directly benefitting from the status quo but also of those driven by ideology, patriotism, or fear of change and, therefore, cut across large segments of society. Such online mobilisation campaigns are employed not only for crowding out the opposition from social networks or organising pro-regime anti-opposition rallies but also to disseminate propaganda more effectively.

Furthermore, SM can have destabilising consequences unrelated to the nature of government. There are indications (particularly from multiethnic states) that penetration of SM has a tendency to instigate collective violence by exacerbating group differences, especially when online networks are formed along segregated lines. SM can also have a destabilising effect by causing dissatisfaction with democracy through raising impossible demands or through exposition to widespread disagreement on fundamental issues. Both of these traits can also be used in what later will be referred to as influence operations.

From the above, it is clear that SM’s track record so far has been far from unequivocal. Indeed, the relationship between SM and political change is “complex and contingent” and SM does not seem to possess any intrinsic quality that exclusively leads
to democratisation. Rather, one has to recognise the contingent nature of SM. It can be very useful and effective in organisation, dissemination of information, and radicalisation (in the sense of increasing the willingness to stand up for a cause). The issue is that all of these processes can work in both positive and negative ways. SM also cannot cause revolutions on its own. In fact, two elements are needed. First, any movement needs a core of hard-line devotees who prepare the information and carry out the initial dissemination. SM activism seems to be dominated by those who are already active in the offline environment, people associated with conventional politics, and a limited number of influential bloggers – professional influencers. It is up to them to turn a particular SM-based movement in a direction of their choice. Second, there must be a set of grievances and other motivations that turns online potentiality into offline actuality. Notably, “[t]here is no positive correlation between levels of SM penetration and the emergence of social movements calling for political reform and regime change”; instead, local political and socio-economic conditions with regards to democracy are the key. Overall, the actual (democratic or anti-democratic) effect of SM depends on both the intention of the initiators and on the nature of offline conditions.

Influence Operations and the Hybrid War in Ukraine

The second part of the article endeavours to demonstrate the ways in which the empowering and mobilising features of SM can be used in a strategic manner to affect the perceptions and actions of target populations. After outlining the nature and typical technique of such operations, the conflict in Ukraine will serve as an example.

To begin with, due to their contingent nature, SM is prone to influence operations, carried out by state or non-state actors, whence “[h]oaxes and scare-mongering campaigns seek to subvert public order, then generate and exploit the resulting chaos.” SM influence operations in particular are characterised by “[t]he use of social interactions to mobilize populations without a physical presence,” thus causing ‘individuals or masses of people to spontaneously move in specific ways in response to messaging.’ The ubiquitous nature of cyberspace also means that “hundreds of millions of people can be approached, simply and at a low cost.” These characteristics make SM influence operations a dangerous addition to an adversary’s arsenal.

There are some crucial structural and psychological underpinnings to such use of SM. Notably, SM now is “a unique information source to deal with information- and cognitive-overload problems,
find answers to specific questions, and discover more valuable opportunities for social and economic exchange.”

However, since people tend to connect with others that are similar, such SM use might well lead to ghettoisation and facilitate influence operations. Furthermore, it is common for a large number of mutual contacts to create an interconnected network where not only user A knows user B who knows user C but also user A knows user C; this clustering produces an echo effect, in which user A receives the same information from different directions, thus getting the impression that everybody is talking about it and having the same opinion; hence, a message is further stabilised as truth.

Such influence operations are, essentially, struggles over a narrative about a given country, its population, and government – and even narratives that otherwise appear stable can be dislodged by strong campaigns. From the perspective of the attacker, the aim is to erode trust among members of the society and between the citizenry and the government. Since trust, in its political dimension, reflects the attitude towards one’s society in general, once trust is eroded, any hostile action becomes much easier to carry out. While such strategy is far from new, with the advent of SM, this struggle has become ever more intense and ubiquitous.

Another dangerous aspect of a cyber influence campaign is that once started, it is able to largely continue on its own with the help of the individuals it has already affected. The scheme is as follows: 1) an operation is initiated by a hostile actor; 2) part of the target group is affected by the message; 3) the affected individuals themselves become the generators and disseminators of the influence operation. Such unwitting agents could be referred to as “sofa warriors.” In contrast to derogatory terms, such as “armchair activists” or “slacktivists,” these individuals, while not posing significant danger on their own, are capable of making impact when herded into a social botnet (to borrow a conventional cyber security jargon term). Of course, these botnets of “sofa warriors” must be occasionally prompted, nudged, and kept excited; nevertheless, the work of the initiator is still made significantly easier while the potential reach of the operation increases exponentially due to the significant increase in the number of disseminators.

Furthermore, the strategic aims of an operation have changed. Notably, in case of influence operations, “[t]he win, especially against irregular adversaries, is in the form of political victory” as “[t]he center of gravity is public opinion.” After all, not only national but also “[g]lobal public opinion
is becoming more strategic," with interest-based communities, coalesced around an issue pertinent to a certain country, attracting members around the world, as it were, temporarily expanding that nation’s citizenry. This also means that influence operations are not exclusive to a period of conflict. In fact, they predate the conflict because any anti-state disturbance indicates that the official narrative has already failed to reach or convince a section of the population. Whoever has attempted to take grip on part (or whole) of that state has already succeeded at the cognitive level.

Influence operations are neither self-serving nor, in most cases, self-sufficient: they have to be used to prepare ground for or in conjunction with other means. Most prominently, hostile actions on SM form part of hybrid war. In a hybrid war, the population itself is the battleground with both conventional and informational operations being aimed at accumulating support. In this context, SM, and cyberspace generally, are important in forging and maintaining regional and transnational linkages, facilitating recruitment, and disseminating propaganda; they can also be the site of adversarial efforts to suppress such use. The conflict in Ukraine has been precisely a hybrid one: “a conflict waged by commandos without insignia, armored columns slipping across the international border at night, volleys of misleading propaganda, floods of disinformation” – something that has been part of the Russian military doctrine at least since 2013. And, since any definitions in this kind of conflict are blurred, it is still not entirely clear what the best response is; after all, hybrid challenges “cannot be deterred by troops, tanks and aircraft alone.”

In more concrete terms, the influence operation, coming from Russian-controlled or backed media, has been aimed at creating an image a ‘humanitarian crisis’ in Eastern Ukraine and portrayal of Ukrainians as Nazis, wearing swastikas and carrying out something akin to a genocide of Russian speakers. Consequently, the Ukraine conflict has also become “a battle of narratives” in which SM is used to spread graphic images of violence, often “borrowed” from other conflicts (Syria, Chechnya, Bosnia etc.). To that extent, an “invisible, clandestine army” of “social networkers, rumor-mongers, and the armies of trolls” are claimed to be an “indispensable weapon” in the Russian strategy to portray the Ukrainian conflict as a defence of Russian-speakers from neo-Nazi mobs and atrocious Ukrainian army. Notably, since the Russian media were banned in Ukraine after the fall of President Yanukovich, SM became the prime vehicle to mo-
bilise pro-Russian groups within the society, essentially creating parallel information realities. Not surprisingly, this has been, according to NATO's Supreme Allied Commander in Europe General Philip Breedlove, ‘the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare’. Clearly, this conflict has disclosed SM’s potential for distortion, whence populations are caught in a torrent of partial information and only pick those bits and pieces that either neatly slot into their preconceptions or provoke their emotions sufficiently. After all, if a message has become viral and is being repeated sufficiently, it is no longer questionable. Crucially, once competing influence operations have reached a critical mass of self-perpetuation and increased radicalisation, any feasible solution becomes less and less likely: the “sofa warriors” on both sides begin living in parallel informational universes with (almost) no common vocabulary – and that has been precisely the lesson of the Ukraine conflict.

Conclusions

Although SM has, for some time already, been mooted as the most important game-changer for pro-democracy movements, the evidence is contradictory. This points to a nuanced take on SM: it 1) does not have a distinctive democratising quality of its own and is 2) insufficient to instigate action without appropriate offline conditions. What is clear is that the contingent nature of SM does allow for its exploitation in influence operations, whereby hostile actors aim to manipulate the population into pre-programmed ways of acting. Admittedly, employment of SM in perception management and orchestration of large-scale demonstrations might not be an all-encompassing tactical tool but it can certainly be used as part of overall strategy. After all, “hybrid actions are all the more powerful […] when backed by the credible threat of force,” as is evident in Ukraine.

In the face of hybrid warfare, there is a need for NATO and other organisations to brace themselves for hostile influence operations and, arguably, acquire the capabilities of carrying out campaigns of their own. Crucially, weaponised SM information has become part of the security landscape. Moreover, it is vital to recognise that influence operations (including defensive ones) cannot be limited to offline military conflicts – they must be permanent.
issues of political ordering, primarily concentrating on the tensions between the constituent and the constituted power in modern democracies; (2) international political theory, especially the history and practice of sovereignty and modern challenges to sovereignty; (3) cyber security, cyber regulation, and political use of social media; 4) more generally, formation of political groups and identities. Ignas’ most recent publications analyse the tensions between sovereignty and universal norms and symbolic representations of social media.

NOTES
2 Collings, Deirdre and Rohozinski, Rafal, Bullets and Blogs: New Media and the Warfighter (US Army War College, Centre for Strategic Leadership, 2009), 5.
7 Merlyna Lim, ‘Many Clicks but Little Sticks: Social Media Activism in Indonesia’, Journal of Contemporary Asia, 43(4) (2013): 638.
17 Jeffrey S. Juris, ‘Reflections on #Occupy Movement’.
28 Gunitsky, ‘Corrupting the Cyber-Commons’.
31 Andrea Ceron and Vincenzo Memoli, ‘Flames and Debates: Do Social Media Affect Satisfaction with Democracy?’, Social Indicators Research (published online ahead of print on 8 February 2015, DOI: 10.1007/s11205-015-0893-x).
32 Ibid.
34 Lim, ‘Many Clicks but Little Sticks’.
36 Loader and Mercea, ‘Networking Democracy?’, 761.
37 Tim Markham, ‘Social Media, Protest Cultures and Political Subjectivities in the Arab Spring’, Media, Culture & Society, 36(1) (2014): 89-104; Reuter and Szakonyi, ‘Online Social Media and Political Awareness in Authoritarian Regimes’.
tack (Office of Naval Research 2013), 4
40 Panayotis A. Yannakogeorgos, ‘Re-
thinking the Threat of Cyberterrorism’, in
Thomas M. Chen, Lee Jarvis and Stuart
Macdonald (eds.) Cyberterrorism: Under-
standing, Assessment, and Response
(Berlin and Heidelberg: Springer 2014), 57
41 Ibid., 57.
42 Heickerö, Roland, Dark Sides of the
Internet: On Cyber Threats and Informa-
tion Warfare (Frankfurt am Main: Peter
Lang, 2012): 154; see also Timothy L.
Thomas, ‘Hezbollah, Israel, and Cyber
43 Daniel Zeng, Hsinchun Chen, Robert
Lusch and Shu-Hsing Li. ‘Social Media An-
alytics and Intelligence’, IEEE Intelligent
44 J. Pfeffer, T. Zorbach and K. M. Carley,
‘Understanding Online Firestorms: Neg-
ative Word-of-mouth Dynamics in Social
Media Networks’, Journal of Marketing
45 Joseph, ‘Social Media, Political
Change, and Human Rights’, 175.
46 Pfeffer, Zorbach and Carley, ‘Un-
derstanding Online Firestorms’.
47 Laura Roselle, Alister Miskimmon and
Ben O’Loughlin, ‘Strategic Narrative: A
New Means to Understand Soft Power’,
48 See e.g. Erika van Elsas, ‘Political Trust
as a Rational Attitude: A Comparison
of the Nature of Political Trust across
Different Levels of Education’, Political
Studies (published online ahead of print
on 30 June 2014, DOI: 10.1111/1467-
9248.12148); Elizabeth Ivarsflaten and
Kristin Strømsnes, ‘Inequality, Diversity
and Social Trust in Norwegian Commu-
nities’, Journal of Elections, Public
Opinion and Parties, 23(3) (2013): 322-
342; Mark Hooghe, Sofie Marien and
Thomas de Vroome, ‘The Cognitive Basis
of Trust: The Relation between Educa-
tion, Cognitive Ability and Political Trust’,
49 See, notably, Evgeny Morozov, The
Net Delusion: The Dark Side of Internet
50 Collings and Rohozinski, ‘Bullets and Blogs’, 2.
51 P.J. Crowley, ‘The Rise of Trans-
parency and the Decline of Secrecy
in the Age of Global and Social Media’, Penn State Journal of Law & In-
ternational Affairs, 1 (2012), 259.
52 Anthony Stefanidis et al., ‘Demar-
cating New Boundaries: Mapping
Virtual Polycentric Communities
Through Social Media Content’, Car-
tography and Geographic Information
53 Warren, ‘Not by Sword Alone’.
54 John J. McCuen, ‘Hybrid wars’, Mili-
55 Josef Schroefl and Stuart J.
Kaufman, ‘Hybrid Actors, Tactical
Variety: Rethinking Asymmetric and
Hybrid War’, Studies in Conflict &
56 ‘Russia's New Tactics of War Shouldn't
Fool Anyone’, Washington Post, 27
washingtonpost.com/opinions/russias-
new-tactics-of-war-shouldnt-fool-any-
one/2014/08/27/0cb73b3a-2e21-11e4-
9b98-848790384093_story.html (accessed
26 February 2015); see also Robin Niblett,
‘NATO Must Focus on the “Hybrid Wars”
Being Waged on the West’, Chatham
www.chathamhouse.org/expert/com-
57 Sam Jones, ‘Ukraine: Russia's new
art of war’, The Financial Times,
www.ft.com/cms/s/2/ea5e82fa-2e0c-
11e4-b760-00144feabdc0.html#ax-
zz3DY0H17Rn (accessed 26 October
2015); see also ‘From Cold War to Hot
War’, The Economist, 14 February 2015,
com/news/briefing/21643220-rus-
sias-aggression-ukraine-part-broad-
er-and-more-dangerous-confronta-
58 ‘Hybrid War – Hybrid Response?’,
www.nato.int/docu/review/2014/
Russia-Ukraine-Nato-crisis/Rus-
sia-Ukraine-crisis-war/EN/index.
htm (accessed 26 February 2015).
59 Niblett, ‘NATO Must Focus on the
“Hybrid Wars” Being Waged on the West'.
68 Niblett, ‘NATO Must Focus on the “Hybrid Wars” Being Waged on the West’.

Title Page Photo by: Jason Howie