BIISS JOURNAL, VOL. 40, NO. 4, OCTOBER 2019: 369-393

Ayesha Binte Towhid

WEAPONIZATION OF SOCIAL MEDIA AND NATIONAL SECURITY

Abstract

In the age of information, social media has emerged as an exponential source of power for people and for the states. In contemporary times, the use of these platforms by the states and state-backed actors have gained prominence in the security studies discourse. As part of the changing character of warfare and foreign intervention, the states have been in the quest of innovative, effective and convenient ways to exert influence and to achieve political and strategic goals. Social media turned out to be an effective tool for this, as several features of social media applications made it possible to reach and target people, communities and institutions of another country instantly, affordably and in a very concealable manner. This opportunity instigated the states and state-backed agencies to weaponize social media for sponsoring information warfare or influence operations in the target states. The present paper analyzes how the use of social media in Russian information warfare against the United States (US), Europe and Africa, and Iran's operations in the US, United Kingdom (UK), Latin America and the Middle East affected the critical political and social institutions, manipulated public opinions, and challenged the territorial integrity and ideologies. It also infers a connection between the evolving weaponization of social media and national security to understand how a country can use social media to threaten the national security of another country.

Keywords: Social Media, Information Warfare, Influence Operation, Foreign Interference, National Security

1. Introduction

Founded on the premise of facilitating communication among peers, social media has come a long way since its creation. It not only revolutionized communication but also became an integral part of almost all spheres of people's lives. Social media became the platform for governments to interact with citizens, for politicians to promote their campaigns, for activists to connect with likeminded people, for businesses to advertise their products, for entrepreneurs to create a clientele, for professionals to network, for students to access educational materials, for celebrities to reach out to their fan following and for everyone to speak their minds. With several hundred social media applications and millions of people

Ayesha Binte Towhid is Research Officer at Bangladesh Institute of International and Strategic Studies (BIISS). Her e-mail address is: ayesha@biiss.org.

accessing it every day, social media blurred the line between the real and virtual world. Today the leading social media companies are valued in billions of dollars. With 2.45 billion monthly active users as of the third quarter of 2019[1], the social media giant Facebook is now one of the five most valuable listed firms in the world.[2] If data is to this century what oil was to the last one,[3] then social media companies are one of the key players as a large portion of data is generated by the users of social networks. This shows the magnitude of social media's influence on people and the power and opportunity it offers to its users.

But this unparalleled power and opportunity of social media have not always been positively used. Social media has been subjected to misuse by various groups to gain detrimental interests. Initially, it was misused by disorganized groups for activities like impersonation, blackmailing, deception, circulation of misinformation and promotion of hate speech, etc. But gradually, it became subjected to misuse by organized groups. Social media became instrumental in the recruitment and promotion strategy of radical and terrorist organizations. With tailor-made content for the target groups, Islamic State of Iraq and Syria (ISIS) used several features of social media sites to reach, communicate and infiltrate minds with radical ideologies. The extent and effectiveness of this use seemed to have outpassed all previous strategies of terrorist organizations. Cambridge Analytica added an entirely new dimension to the misuse of social media. By harvesting data to create psychological profiles of consumers and voters, the company changed the way of designing online political campaigns. The data breach of Cambridge Analytica opened up intense debates regarding social media companies and user data protection. Social media was also extensively used by the major political parties in several countries to push specific narratives to different groups based on their social and political preference to persuade them before crucial decision-making like elections and referendum. While these issues indicated critical societal and political challenges to the government and policymakers, the challenge became further intensified when the foreign state and state-backed agencies began to use social media as a weapon grade communication tool to threaten the core elements of a target state.

The issue of weaponizing social media[4] came in the limelight after revelations

[1] J. Clement, "Number of monthly active Facebook users worldwide as of 3rd quarter of 2019", available at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/, accessed on 15 December 2019.

[2] "The world's most valuable resource is no longer oil, but data", *The Economist*, 06 May 2017.

[3] "Data is giving rise to a new economy", *The Economist*, 06 May 2017.

[4] Weaponization of social media specifically highlights the use of social media as a tool of information warfare. The paper denotes that social media is to be considered as a national security concern only when foreign states and state-backed agencies abuse the technology of the platforms in information warfare to secure political and strategic interests in target countries by interfering in their internal affairs. Other forms of uses and abuses of social media are outside the purview of this paper. The term "Weaponization of Social Media" has been

of Russian alleged interference in the 2016 United States (US) elections. However, this was not the first attempt of social media weaponization. Russia parallelly ran influence operations in many countries in Europe and very recently expanded to Africa. Iran was also quick to adopt similar techniques of using social media to secure political and strategic goals in regions of its interest like the Middle East and Latin America and in countries like the US and UK. There is a growing suspicion that more countries are resorting to this aspect of using social media.[5] In this context, using the state as the level of analysis, the paper attempts to qualitatively study how state and state-backed agencies weaponize social media to conduct information warfare or influence operations and assess how the core elements of a state are affected by this process. It then relates these threats to core elements of a state through the weaponization of social media by foreign actors with the concept of national security and evaluates whether this issue can be considered as a national security threat.

The rest of this paper has been organized as follows. The second section chalks out a conceptual framework to understand the technological features of social media, the inclusion of social media in information warfare, concepts of national security and analysis of national security threats. The third section presents three key cases of weaponization of social media based on reports and analysis of the data provided by social media firms to the US Senate Select Committee on Intelligence (SSCI), disclosures of Facebook and Twitter and study of reputed cybersecurity firms and internet institutes. The fourth section develops a qualitative assessment of the cases and identifies which core components of a state were affected by the weaponization of social media, how it has been securitized and whether this issue can be considered as a national security threat. The fifth section concludes the paper.

2. Conceptual Framework

While the word 'social media' is regularly used in everyday lives, there are only a few definitions to clearly set the boundary of this new media. Andreas Kaplan and Michael Haenlein defined social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content".[6] The

frequently used in describing this particular kind of social media's strategic use.

[5] Twitter Safety, "Disclosing new data to our archive of information operations", available at https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html, accessed on 05 December 2019; Twitter Safety, "Information operations directed at Hong Kong", available at https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html, accessed on 05 December 2019; Nathaniel Gleicher "Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan", available at https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/, accessed on 27 January 2020.

[6] Andreas Kaplan and Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of

term includes, but not limited to, social networking sites, mobile applications and information and content sharing sites. In this paper, social media primarily refers to the most frequently used applications, i.e., Facebook, Twitter, Instagram, YouTube and VKontakte whose misuses have given rise to national security threats. These social media applications created scopes to have maximum reach and impact with limited time, effort, expense and risk. With their numerous user-friendly features, social media applications made it possible to instantly reach out to any corner of the world, create multimedia content, amplify the contents with bots, micro-target people, harvest user data, build psychological profiles and manipulate each audience differently through separate and customized narratives which might resonate best with them. While most of these services were designed for digital advertisers, the state and state-backed agencies weaponized these techniques to secure political and strategic interests. This has been primarily done by incorporating social media in the toolkit for influence operation and information warfare.

State-sponsored propaganda and information warfare have always been an integral tool for foreign interference. Interchangeably used with information operations or influence operations, information warfare involves the collection of tactical information about an adversary as well as the dissemination of propaganda to achieve a competitive advantage over an opponent.[7] One of the most prominent examples of state-backed propaganda is Operation Infektion orchestrated by Komitet Gosudarstvennoy Bezopasnosti (KGB) to spread that AIDS was created by the CIA.[8] Similar Soviet propaganda efforts included KGB sending forged racist letters in the name of the Ku Klux Klan threatening twenty athletes from Asian and African nations in the 1984 Summer Olympics[9], circulating false reports that the US was bringing Latin American children to harvest their organs for organ transplants[10], a campaign with fake documents insinuating that the US government supported apartheid, etc.[11] This series of influence mechanisms called 'active measures' which began in the Soviet era, gradually became a well-established Russian tactic. Such tactics of information warfare continued to evolve based on the expansion of technology, political objectives and target countries. The Russian Federation Armed Forces' Information Space Activities Concept, defines information warfare as the

Social Media", *Business Horizons*, Vol. 53, No. 1, January-February 2010, p. 61.

[7] "Information Operations", RAND Corporation, available at https://www.rand.org/topics/information-operations.html, accessed on 15 November 2019.

[8] Thomas Boghardt, "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign", *Studies in Intelligence*, Vol. 53, No. 4, 2009, p. 2.

[9] Fred Barbash, "US Ties 'Klan' Olympic Hate Mail to KGB", *Washington Post*, 07 August 1984.

[10] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Strategic Perspectives*, Vol. 11, 2012, p. 63.

[11] Renee DiResta and Shelby Grossman, "Potemkin Pages & Personas: Assessing GRU. Online Operations, 2014-2019", Working paper, Stanford: Stanford Internet Observatory, 2019.

confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society as well as coercion of the state to take decisions for the benefit of the opposing force.[12] Gradually more countries adopted this technique, tailored it as per their objectives and used it at different times to influence thoughts and opinions to secure political and strategic objectives in a target country.

This strategy of using information as a weapon is now more relevant than ever as the twenty-first century is witnessing major changes in the character of warfare and foreign intervention. It is a time in which wars are not always declared and when initiated, it often proceeds in an unfamiliar pattern.[13] It is also a period in which there has been an increasing effort to use non-military means to exert influence and achieve political and strategic goals in another country.[14] In this circumstances, social media applications emerged as an ideal vector of information attacks.[15] The combination of such digital communication tools with the changing nature of warfare made social media a topic of discussion in national security.

National security can be equated with the survival of the state and its relative freedom from existential threats. The Encyclopaedia of the Social Sciences defines national security as "the ability of a nation to protect its internal values from external threats." Giacomo Luciani defined national security as "the ability to withstand aggression from abroad."[16] While this definition can be considered as a starting point for conceptualizing national security, the idea has been debated, widened and deepened in different phases based on the referent object and the threats surrounding it.

Traditionally, the state is viewed as the referent object of security policy and it is perceived that the state sovereignty and territorial integrity must be protected from military threats of an aggressive state actor which seeks to attack, destroy or capture the state for their purpose.[17] Here, the primary concern is safeguarding the

[12] Ministry of Defense of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept*, Moscow: Department of the Ministry of Defence of the Russian Federation for Citizens Affairs, 2012.
[13] Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations", *Military Review*, January-February 2016, p. 24.
[14] Ibid.
[15] Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security", California: RAND Corporation, 2017.
[16] Alan Collins, "Introduction", in Alan Collins (ed.), *Contemporary Security Studies*, UK: Oxford University Press, 2013, p. 3.
[17] Leanne Jennifer Smythe, *Non-traditional security in the post-Cold War era: implications of a broadened security*

state from external military threats. External threats can come in diverse forms and constantly evolve. Barry Buzan analyzed these threats based on few sectors like military, political and economic. Military threats threaten all the components of state. It can cause strain, damage and dismemberment to the physical base of the state, distort or destruct the institutions and also repress, subvert or obliterate the idea of state.[18] Besides striking these protective functions of the state, military threats can also threaten and damage deep down through the layers of social and individual interests.[19] However, he opined that military threats do not necessarily have to be in the extreme end of invasion and occupation, it can also aim to alter institutions and ideology of the state. Barry Buzan noted that military threats can also have political objectives. These political objectives are often pursued politically which involves targeting the idea of the state, its organizing ideology, the institutions which express it and manipulation of its policy or behaviours.[20] Political threats can be critical for the states where the ideas and institutions are already internally contested as in these cases the states are highly vulnerable to political penetration. Such threats stem from the battles of ideas, information and tradition and the interplay of these ideas and communication can produce politically significant social and cultural threats.[21] Barry Buzan also mentioned about indirect threats which do not directly apply to the state, instead, it is directed to its external interests. This analysis of external threats is used in this paper as one of the dimensions of assessing the threats pertaining to the weaponization of social media by the foreign states and state-backed agencies.

Till the end of the Cold War period, the concept of national security considered state as the referent object and securing it from external attacks was dominant among statesmen and security apparatus. While in the post-Cold War era, the strategic environment changed and there were demands to make security inclusive of new threats and insecurities experienced by the state and the people within the state. This led to the broadening and deepening of the traditional concept of security. The non-traditionalists conceptualized security in regards to non-military threats directed towards both the states and societies.[22] Along with many new issues, non-military threats included emerging risks pertaining to information technology and cyberspace. In this circumstance, the concept of cybersecurity came into focus. However, the concept of cybersecurity has also witnessed a fair share of changes over the past three decades. Initially, cybersecurity was viewed by governments and policymakers as a technical issue. In the 1990s, militaries began to gradually treat

agenda for the militaries of Canada and Australia, Vancouver: University of British Columbia, 2013, p. 12.

[18] Barry Buzan, *People, states, and fear: The national security problem in international relations*, North Carolina: University of North Carolina Press, 1983, p. 75.

[19] Ibid. p. 75.

[20] Ibid. p. 76.

[21] Ibid. pp. 75-77.

[22] Leanne Jennifer Smythe, op. cit.

cyberspace as a domain of warfare in theory and practice.[23] The situation started to escalate in the 21st century as the world witnessed a series of major attacks in cyberspace which included global ransomware attack, Denial of Service (DoS) attacks, privacy breach, data leaks and attacks on national web assets, nuclear facility, steel plant and power grids.[24] The proliferation of Information and Communication Technologies (ICTs) in almost all parts of the world in this period made it possible to inflict unprecedented damage. The magnitude of this threat was reflected in the 2008 Russo-Georgian conflict over South Ossetia, where private computing power was organized and coordinated to have a strategic effect on the opponent. Security experts described this coordinated attack as the coming of age of a new dimension of warfare and it showed an untapped potential for using the internet to cause mass confusion for political gain.[25] Soon cyberspace became regarded as the fifth domain of warfare, next to land, sea, air and space.[26] Gradually, both the state and non-state actors began to emphasize more on the internet to secure strategic objectives. However, instead of addressing both the state and non-state actors, this paper would exclusively focus on the use of cyberspace from the state level.

The focus on internet and inclusion of cyberspace in warfare allowed states to explore effective and convenient platforms for pushing forward its strategic interests. With its several tools and features, social media emerged as a natural fit for this strategy. Thus, the state and state-backed agencies began to use social media exclusively or in combination with other mediums to advance their national and strategic interest in target countries and regions. Based on this framework of the evolving nature of national security threats and adopting the realist perspective, the paper attempts to study some key cases of weaponization of social media by the state and state-backed agencies, assesses the implications of social media-based influence operation on core components of a state and relates it with the concepts of national security.

3. Cases of Weaponization of Social Media

To understand how the state and state-backed agencies weaponize social media to conduct information warfare or influence operations, what are the tools and tactics deployed in this method and how target countries are affected, some of the recent cases of weaponization of social media are analyzed in this section based

[23] Myriam Dunn Cavelty and Andreas Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, Vol. 41, No. 1, 2020, p. 15.
[24] Office of Information and Communication Technology, "Digital Blue Helmets", available at https://unite.un.org/digitalbluehelmets/, accessed on 01 December 2019.
[25] Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom Threats and Responses*, London: Chatham House, 2009.
[26] Carmen-Cristina Cirlig, "Cyber defence in the EU: Preparing for cyber warfare?", available at http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf, accessed on 10 November 2019.

on the study of reputed cybersecurity firms, internet institutes and disclosures of Facebook and Twitter.

3.1 *Case 1: Russian Alleged Information Operation in the US*

Information operations have been a major part of Russian foreign policy.[27] This strategy for foreign interference has constantly evolved based on the advancement of technologies and the development of new mediums of communication. Contemporary cases of information operations show the country has mastered the art of incorporating social media in state-led information activities.[28] The magnitude of this operation came in the limelight after the revelation of Russian interference in the 2016 US Presidential elections. The Office of the Director of National Intelligence stated that the assessment of the Central Intelligence Agency, Federal Bureau of Investigation and National Security Agency of the US revealed that Russia undertook an extensive operation to influence the US presidential elections, blending cyber and information operations backed by social media activity.[29] It is believed that this influence operation was primarily conducted by the Internet Research Agency (IRA) based in St. Petersburg, Russia. According to the US Senate Select Committee on Intelligence (SSCI), the Russian government tasked and supported the IRA' interference in the 2016 US elections.[30]

The IRA, popularly known as a troll farm, is an institution which operates like a sophisticated digital marketing agency in a centralized office environment with over a thousand trained people and is engaged in round-the-clock influence operations.[31] IRA is regarded as responsible for planning and executing the influence operation targeting to divide American society, undermining the integrity of the elections process in the US and eventually manipulating public opinion. The Oxford Internet Institute analyzed the data on IRA provided to the US SSCI by the social media and internet platforms to understand the operation strategy. Their research found that IRA began to focus on the US in 2013, initially by using Twitter but it quickly adopted a multi-platform strategy involving Facebook, Instagram and

[27] Todd C. Helmus, Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega and Zev Winkelman, *Russian social media influence: Understanding Russian Propaganda in Eastern Europe*, California: RAND Corporation, 2018.
[28] Ibid.
[29] Ibid.
[30] US Senate Select Committee on Intelligence, "Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaign and Interference in the 2016 US Elections, Volume 2: Russia's Use of Social Media with Additional Views", Washington, D.C.: US Senate Select Committee on Intelligence.
[31] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright and Ben Johnson, "The Tactics & Tropes of the Internet Research Agency", available at https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf, accessed on 02 November 2019.

YouTube amongst other platforms. From the quantitative and qualitative assessment of the social media data, it was found that there was a sustained effort to manipulate the US public and undermine democracy.[32] In order to realize its objectives in the US, the IRA used several features of different social media platforms to produce, promote and engage content for specific target groups. Micro-targeting social media users based on location, race and ethnicity and pushing customized and contradictory content for each of these groups helped IRA sow divisions in the society and manipulate each group's opinion differently. Bots and botnets were extensively used to boost such contents and continuously flood the target audience's newsfeed. It is also believed that IRA members pretended to be US citizens and engaged in discussions to direct the conversation in a way that suited their agenda. They also purchased political advertisements on social media in the names of US persons and entities to boost their reach out. Many people were persuaded by the posts and they themselves promoted the contents without knowing the objectives behind it. Thus, both organic and automated tactics were involved to make the influence operation look credible, convincing and trending.

The scale of this operation was unprecedented. It started by targeting American society in general but as the Presidential contest intensified, the influence operation began to target different social, political and racial groups with specific agendas. In democratic elections, it is important that the decision-making process is inclusive, participatory and representative but by analyzing the data related to this operation, it was found that IRA targeted the American population with differential messaging in social media to push and pull them in different ways. The Oxford Internet Institute's study on Social Media and Political Polarization in the United States revealed that in the 2016 elections, the African American voters were encouraged to boycott elections or follow the wrong voting procedures. Through the ad manager feature in Facebook, IRA targeted African Americans in key metropolitan areas with well-established black communities and flashpoints in the Black Lives Matter movement and continuously shared content regarding the structural inequalities faced by African Americans with the intention to prey on their anger, divert them away from the elections and lose their trust in political institutions. Cases of police violence, poverty and disproportionate levels of incarceration were strategically used in creating ads and messaging for this specific group of voters.[33]

While the IRA campaign discouraged Africa Americans from the elections, reports showed that it encouraged extreme right-wing voters to be more

[32] Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly and Camille François, *The IRA, Social Media and Political Polarization in the United States, 2012-2018*, Oxford, UK: Project on Computational Propaganda, 2018.
[33] Ibid.

confrontational. Right-targeted accounts were fear mongered about voter fraud and warned that the elections would be stolen and violence might be necessary. Oxford Internet Institute's analysis found that messaging to these conservative voters sought to do three things: repeat patriotic and anti-immigrant slogans; elicit outrage with posts about liberal appeasement of 'others' at the expense of US citizens and encourage them to vote for the presidential candidate Donald Trump. Messaging to this segment of voters focussed on divisive and at times prejudiced and bigoted, statements about minorities, particularly Muslims.[34] This strategy showed that through the information operation, there was an intention to polarize the US population and manipulate their decision.

Attempts to polarize the US population was further reflected in the posts regarding the political candidates. IRA's social media content during the 2016 elections reflected clear support for one camp and lack of it for another. According to the finding of the US SSCI , the IRA sought to influence the 2016 US presidential elections by harming Hillary Clinton's chances of success and supporting Donald Trump.[35] The bias for candidate Donald Trump was visible from the early days in the campaign and throughout the entire elections data set provided by social media companies. Alternatively, there was a substantial portion of political content articulating anti-Hillary Clinton sentiments among both Right and Left-leaning IRA-created communities.[36] In short, conservative voters were actively encouraged to support candidate Donald Trump, other voters were encouraged to boycott the elections, abstain from voting for candidate Hilary Clinton and cynicism about participating in the elections, in general, was spread.[37]

Besides targeting political candidates, swing states were targeted as well. Swing states have always been crucial factors in the US elections and this was also used as a part of IRA's tactic. From the data shared by the social media companies, it was found that out of 1,673 instances of location targeting, swing states were targeted 543 times in total.[38] Content analysis showed that average levels of misinformation were higher in swing states.[39] The IRA has also been implicated for promoting secessionist and insurrectionist movements in the US. Influenced by the Brexit activities in UK, content was intentionally created by IRA to promote territorial split and trigger secessionist movements like Texas and California secession, i.e.,

[34] Ibid.
[35] US Senate Select Committee on Intelligence, op. cit.
[36] Renee DiResta et al., op. cit.
[37] Philip N. Howard et al., op. cit.
[38] Ibid.
[39] Philip N. Howard, Bence Kollanyi, Samantha Bradshaw and Lisa-Maria Neudert, *Social Media, News and Political Information during the US Elections: Was Polarizing Content Concentrated in Swing States?*, Data Memo No. 2017.8, Oxford, UK: Project on Computational Propaganda.

(#texit) and (#calexit).[40] Actions like this from a foreign entity are perceived as a threat to the territorial integrity of a state. Policies were also criticized as part of IRA's attempt to divide the people. Allegations of poor treatment of veterans by the Obama administration was often reflected in the social media content and compared to the well treatment of refugees.[41] There were also attempts to increase division among liberals and conservatives surrounding the issues of lesbian, gay, bisexual and transgender (LGBT). The Muslim Americans were targeted by using the US foreign policy to create suspicion about the American government.[42] This goes into showing the magnitude of the information operation targeting several aspects of the American society and institutions.

The data produced in front of the US SSCI showed that between 2014 and 2017, IRA reached 126 million people on Facebook, at least 20 million users on Instagram, 1.4 million users on Twitter and uploaded over 1,000 videos to YouTube.[43] The US special counsel Robert Mueller announced in September 2018 that 13 Russians and three Russian entities, including the IRA, had been indicted by a federal grand jury in Washington DC.[44] The indictment revealed that the defendants allegedly conducted what they called "information warfare against the United States," with the stated goal of "spread[ing] distrust towards the candidates and the political system in general" and social media was used in different phases of this process.[45]

However, the information operation did not stop even after IRA was caught interfering in the 2016 elections. Capitalizing on President Donald Trump's viewpoints on Mexican American, IRA seems to have made this community a new target of its information operation. The IRA ran campaigns repeating the same themes as with African American voters. The campaigns were geared towards increasing distrust and cynicism about the US political system and issues such as discrimination, deportation and treatment of migrants were reflected in the social media content targeted towards this group.[46] Oxford Internet Institute's study showed that besides targeting this specific group, IRA continued its social media engagement targeting American societies in general and covered a widening range of public policy issues, national security issues and issues pertinent to younger voters,

[40] Renee DiResta et al., op. cit.
[41] Philip N. Howard et al., op. cit.
[42] Ibid.
[43] Renee DiResta et al., op. cit.
[44] Jon Swaine and Marc Bennetts, "Mueller charges 13 Russians with interfering in US elections to help Trump", *The Guardian*, 17 February 2018.
[45] US Department of Justice, *Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System*, Washington DC: Department of Justice Office of Public Affairs, 2018.
[46] Philip N. Howard et al., op. cit.

which mean the challenge as persistent and likely to intensify in the coming days.

3.2 *Case 2: Russian Alleged Influence Operations in Europe and Africa*

The disclosure of IRA's interference in US elections brought the issue of weaponization of social media in public domain and made it one of the most discussed topics of the present time. However, Russia simultaneously ran influence operations in other parts of the world as well. Russian social media operations seemed to have challenged the national security of many countries in Europe and most recently in Africa. Analysis of the social media strategies showed that it was designed on the basis of Russia's political objectives in the specific target countries.[47]

In Russia's near abroad countries like Estonia, Latvia, Lithuania, Ukraine, Moldova and Belarus, the Kremlin had always aimed to leverage shared elements of the post-Soviet experience in order to drive wedges between ethnic Russian or Russian speaking populations who reside in these states and their host governments.[48] Russia also made social media an integral part of its information operation in this region. It was particularly evident in the Ukraine conflict. Following EuroMaidan and throughout the conflict, Ukraine has been targeted by numerous disinformation campaigns and propaganda efforts, predominantly from Russia.[49] Russia had a strategic advantage in this regard as the popular social media platforms in this region like VKontakte and Odnoklassniki are owned by Russian companies. Thus, Russian attempts to manipulate and influence public opinion during the crisis in Ukraine were possible by controlling these social media platforms. StratCom's March 2015 report uncovered actions of Russian social media operations such as blocking pro-Ukrainian groups and requesting personal information of activists.[50] From the dataset analysis of IRA accounts provided by Twitter, Cardiff University's Crime and Security Research Institute found that over 20 per cent (1022) of the tweets contained clear references to the situation in Ukraine, often referring to Ukrainians being 'fascists' led by a 'murderous junta'.[51] The 2014 Ukrainian elections received special attention from the IRA Twitter accounts and the leading candidate Petro Poroshenko was specifically targeted. IRA generated multiple messages alleging that Petro Poroshenko was a 'stooge' put in place by Western intelligence agencies.[52] A

[47] Todd C. Helmus et al., op. cit.
[48] Ibid.
[49] Mariia Zhdanova and Dariya Orlova, *Computational Propaganda in Ukraine: Caught between External Threats and Internal Challenges*, Working Paper 2017.9. Oxford, UK: Project on Computational Propaganda, 2017.
[50] Ibid.
[51] Crime and Security Research Institute, *The Internet Research Agency in Europe 2014-2016*, Cardiff, Wales: Cardiff University, 2019.
[52] Ibid.

common theme among all the tweets shared during the elections period was that the electoral process was corrupted and candidates were purchasing votes.

In the farther abroad countries, Russian objectives involved achieving policy paralysis by sowing confusion, stoking fears and eroding trust in Western and democratic institutions.[53] Social media was again made instrumental in reaching to the people of these countries in Europe. Studies showed that Russian propaganda efforts were targeted towards establishing a narrative which tarnishes democratic leaders and institutions, erodes confidence in foreign markets and capitalist economies, discredit Western financial experts and business leaders and fear mongers about war.[54] In all of these efforts, digital entities like trolls and bots were extensively used to create a viral effect of the narrative.

The IRA is also believed to have attempted to influence opinion in Germany. Social media content analysis showed that IRA accounts generated multiple and often contradictory narratives to sow chaos and confusion in the country. For example, during high profile debates surrounding the Syrian refugee crisis and Angela Merkel's policy regarding it, IRA accounts took both sides on social media discussions to further escalate the division in the society.[55] In the 2017 German federal elections, Russian propaganda efforts sought to skew the public debate with the aim to weaken citizens' faith in the quality of their political system.[56] In Italy, IRA-linked accounts repeatedly promoted that Italy should leave the European Union (EU), scrap the Euro and quit North Atlantic Treaty Organization (NATO), in order to recover their sovereignty.[57] In Turkey, IRA trolls targeted President Erdogan as well as the general citizens. Content analysis showed that IRA accounts accused President Erdogan of planning the refugee crisis and spread fear about Turkey joining the EU and the movement of people afterwards.[58] It was alleged that Russia used a combination of traditional and social media to undermine Turkey's political and security cooperation with the US and Europe by exacerbating mutual scepticism and highlighting policy differences.[59] Studies showed that the social media campaign in Turkey contributed to anti-American discourse, promoted anti-US conspiracy theories and attempted to create fissures with the West, particularly after the Turkish coup attempt. Here IRA deployed the three primary strategies of information operations, i.e., amplification

[53] Todd C. Helmus et al., op. cit.
[54] Ibid.
[55] Crime and Security Research Institute, op. cit.
[56] Katja Theodorakis and Clint Arizmendi, "Cyber Security in a Contested Age – Geopolitical Challenges and Opportunities for Australia and Germany", *PERISCOPE Occasional Analysis Paper Series*, Vol. 2, Konrad Adenauer Stiftung (Australia), 2019.
[57] Crime and Security Research Institute, op. cit.
[58] Ibid.
[59] Katherine Costello, "Russia's Use of Media and Information Operations in Turkey", RAND Corporation, 2018.

of genuine uncertainty, creation of opportunistic fabrications and use of multiple contradictory narratives.[60]

Similar efforts of weaponizing social media as part of influence operation were also visible in Africa. Russia has been seeking to increase its presence in Africa through several means for the past couple of years. Recently, the country included social media in its strategy. In October 2019, Facebook revealed that it had removed three networks of Facebook and Instagram accounts for engaging in coordinated inauthentic behaviour on behalf of a foreign actor.[61] According to the disclosure, the network originated in Russia and focussed on Madagascar, the Central African Republic, Mozambique, Democratic Republic of the Congo, Côte d'Ivoire, Cameroon, Sudan and Libya. Stanford Internet Observatory's investigation connected these campaigns to entities associated with Russian financier Yevgeniy Prigozhin and Wagner Group. Yevgeniy Prigozhin is known for his association with IRA and Wagner Group is a Russian private military contractor working in several African countries.[62] Analysis of the content showed that some posts promoted Russian policies while others criticized French and American policies in Africa.[63] According to the report of Stanford Internet Observatory, Russian activity and strategies varied by country. For example, in Libya, Russian actors supported two potential future presidential candidates and in Mozambique, the Facebook pages posted content to support the incumbent president and damage the reputation of the opposition.[64]

The social media campaigns of IRA and Wagner Group show that Russia backed agencies have been involved in influence operations in several countries of Europe and Africa and there are speculations that more countries of these regions are likely to be affected. If the Russian strategy in Europe and Africa is compared to that of the US, it can be seen that the operation varied in terms of the medium used, the agency conducting the campaign and the political and strategic interests involved, however, the objective of the influence operation had resemblance. While Twitter and Facebook were dominant in the US, in Europe, platforms like VKontakte and Odnoklassniki were also used frequently. Besides triggering internal divisions and sowing discord in society, Russia also aimed to create fissures in the foreign relations of the targeted European countries, particularly with the West. This shows

[60] Ibid.

[61] Nathaniel Gleicher, "Removing More Coordinated Inauthentic Behavior From Russia", available at https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia/, accessed on 05 December 2019.

[62] Stanford Internet Observatory, "Evidence of Russia-Linked Influence Operations in Africa", available at https://cyber.fsi.stanford.edu/io/news/prigozhin-africa, accessed on 02 December 2019.

[63] Davey Alba and Sheera Frenkel, "Russia Tests New Disinformation Tactics in Africa to Expand Influence", *The New York Times,* 30 October 2019.

[64] Stanford Internet Observatory, op. cit.

both similarity and dissimilarity with the operation in the US. Also, unlike the IRA's predominant role in the US and Europe, Wagner Group is held responsible for the social media campaign in Africa which signifies a notable difference. Although the campaign strategy varied based on the political and social circumstances of the countries, it can be seen that the end goal to manipulate public opinion and attempt to interfere in the internal affairs of countries are reflected in both the cases discussed here.

3.3 *Case 3: Iran's Influence Operations in the Middle East, Latin America, the US and UK*

Besides Russia, another country which is alleged for extensively weaponizing social media to target countries and regions of its interest is Iran. The country has been attempting to use the digital landscape as a means of information warfare for quite some years.[65] In order to dominate the information space of targeted foreign countries, Iran is believed to have begun operating Facebook and Twitter sockpuppets as early as 2010.[66] According to the Atlantic Council's report, the objective of the social media operations was to launder Iranian state propaganda to unsuspecting audiences, often under the guise of local media reports.[67] In 2011, Iran's former Intelligence Minister Heidar Moslehi remarked that Iran does not have a physical war with the enemy, but it is engaged in heavy information warfare with the enemy.[68] Gradually, the information warfare strategy of the country evolved and expanded to regions beyond the Middle East. Iran adopted an elaborate strategy of using social media in its information operations to exert influence in the Middle East, Latin America, US and UK. This strategy was revealed through a series of disclosures from social media companies and analyzed by cybersecurity firms and security experts.

In August 2018, Twitter suspended 770 accounts with potential Iranian origins for engaging in coordinated manipulation on the platform. According to Twitter's official statement, the information operations linked to Iran were potentially backed by the state.[69] Analysis of tweets from these accounts showed that the majority Arabic tweets were primarily used to promote pro-Iranian Arabic language news websites and websites which push the Iranian political narrative

[65] Donie O'Sullivan, "Iran has online disinformation operations, too," *CNN Business*, available at https://edition.cnn.com/2020/01/03/tech/iran-disinformation/index.html, accessed on 12 March 2020.
[66] Emerson T. Brooking, Suzanne Kianpour, *Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century*, Washington DC: Atlantic Council, 2020.
[67] Ibid.
[68] "Iran Adopts Aggressive Approach Toward Enemies," *Tehran Times*, 18 July 2011.
[69] Mona Elswah, Philip N. Howard and Vidya Narayanan, *Iranian Digital Interference in the Arab World*, Data Memo 2019.1, Oxford, United Kingdom: Project on Computational Propaganda, 2019.

including the criticism of Saudi Arabia and support of the Syrian President Bashar al-Assad.[70] The accounts also impersonated popular news outlets to mislead and misinform the audience. In June 2019, Twitter disclosed additional 4,779 accounts originating in Iran and believed those to be associated or directly backed by the Iranian government.[71] Based on the content of the accounts, Twitter divided those into three data sets.[72] The first set consisted of 1666 accounts and through nearly 2 million tweets, these accounts pushed out global news content which had an angle that benefited the diplomatic and geostrategic views of Iran. The second set consisting of 248 accounts was specifically engaged in discussion related to Israel. The third set of 2865 accounts employed a range of false personas to target conversations about political and social issues in Iran and globally.

Besides Twitter, Iran's influence operation was also visible in platforms like Facebook and Instagram. In August 2018, Facebook removed 652 pages, groups and accounts on Facebook and Instagram originating from Iran for engaging in a 'coordinated inauthentic behaviour'. In October 2018, Facebook announced the removal of another 82 pages, groups and accounts on Facebook and Instagram which targeted people in the US and the UK. Some of these accounts masqueraded as American citizens and pushed anti-Saudi and anti-Israel narratives.[73] As part of Facebook's continued effort, in October 2019 the company disclosed the removal of three networks with Iranian origin for engaging in coordinated inauthentic behaviours.[74] The first network contained 93 Facebook accounts, 17 pages and four Instagram accounts which focussed primarily on the US and French-speaking audiences in North Africa. The pages and accounts posted about local political news and geopolitical topics like public figures in the US, politics in the US and Israel, support of Palestine and conflict in Yemen. The second network consisted of 38 Facebook accounts, six pages, four groups and ten Instagram accounts which focussed on countries in Latin America, including Venezuela, Brazil, Argentina, Bolivia, Peru, Ecuador and Mexico. This account repurposed Iranian state media stories on topics like Hezbollah, conflict between Iran and Saudi Arabia, tensions between Israel and Palestine, Iran and the US and war in Yemen. The accounts also posted content tailored for particular countries including domestic news, geopolitics and public figures. The third was a small network of four Facebook accounts, three pages and seven Instagram accounts that focussed mainly on the US and posted

[70] Ibid.
[71] Yoel Roth, "Information operations on Twitter: principles, process, and disclosure", available at https://blog.twitter.com/en_us/topics/company/2019/information-ops-on-twitter.html, accessed on 15 November 2019.
[72] Ibid.
[73] Mona Elswah et al., op. cit.
[74] Nathaniel Gleicher, "Removing More Coordinated Inauthentic Behavior From Iran and Russia" available at https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/, accessed on 03 December 2019.

about political issues, including race relations in the US, criticism of the US and Israel's policy on Iran, the Black Lives Matter movement, African-American culture and the Iranian foreign policy. The cybersecurity firm FireEye summarized Iran's influence operation targeting people in the US, UK, Latin America and the Middle East as an attempt to promote anti-Saudi, anti-Israeli and pro-Palestinian themes as well as support for specific policies favourable to Iran, such as the Iran nuclear deal (JCPOA).[75] This reflects the extent of Iran's influence operation in several parts of the world to push forward its strategic objectives through the weaponization of social media.

Now if the Iranian strategy of weaponizing social media is compared to the Russian strategy, it can be seen that there is a contrast in the type of content manufactured and shared. While Russia's IRA is seen to extensively engage in sharing disinformation, Iran takes a different strategy than disseminating obvious falsehood. Instead, Iran propagates a distorted version of information which exaggerates Iran's moral authority, represents its world view, advances specific foreign policy objectives and minimizes the dissemination of its criticism.[76] Studies showed that Iran's digital influence operations represent a continuation of public diplomacy through misleading websites and networks of fake social media accounts. According to the Atlantic Council's report, if the principal intent of Russia's digital influence efforts is perceived to distract and dismay, Iran's goal is most often to persuade. The report also analyzed that in contrary to Russia's use of clandestine means to play both sides of a political issue against each other, Iran uses clandestine means to amplify one side as loudly as possible.[77] However, in the strategy of both countries, the actors are seen to abuse the technology of social media and manipulate public opinion in countries and regions of their interests.

4. Assessment of National Security Threats

The three cases exemplify the growing trend of weaponizing social media as part of information warfare or influence operation to achieve political and strategic goals in a target country. The cases show the attempt of Russia backed agencies to use social media to interfere in the US, in eight African countries and many European countries including Ukraine, Germany, Italy and Turkey and Iran's influence operation in the Middle East, Latin America, the US and UK. It also shows that

[75] FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in US, UK, Latin America, Middle East", available at https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html, accessed on 10 November 2019.
[76] Emerson T. Brooking et al., op. cit.
[77] Ibid.

starting from the US in 2013 to Africa in 2019, these foreign interference campaigns have expanded in capacity and evolved based on the latest technological features offered by social media applications. In this part, the paper assesses these cases to evaluate if this issue can be regarded as a national security concern.

If national security is considered as the ability of states to protect itself from external threats, it is seen that in all these cases the national security of the target states was challenged by a foreign actor. Foreign actors weaponized social media to interfere in the internal affairs of the state. The use of information operations by foreign actors is believed to have affected the political system. It was threatened by attempts of questioning the electorate process, spreading confusion and doubt, and manipulating public opinion in crucial decision-making processes through social media posts and advertisements. For example, in Ukraine, a common theme among the IRA tweets shared during the 2014 elections was that the electoral process was corrupted and candidates were purchasing votes. In the 2016 US elections, specific groups were targeted with differential messaging like follow wrong voting procedure or boycott the elections. This voter suppression technique on Facebook and Instagram was particularly directed towards the African American communities in the US. According to the finding of the US SSCI, no single group of Americans was targeted by IRA information operatives more than African-Americans.[78] Following the elections, a report from Pew Research Center showed that in 2016, black voter turnout rate in a presidential elections declined for the first time in 20 years, falling to 59.6 per cent from the record-high of 66.6 per cent in 2012.[79] While it is not conclusive that the Russian influence campaign was directly responsible for this decline, the pattern in which IRA consistently targeted this community on social media is quite likely to have an impact on their decision to vote. In the 2017 German federal elections, Russian propaganda efforts also sought to weaken citizens' faith in the quality of their political system. Peter Pomerantsev and Michael Weiss assessed the Russian influence operation as an attempt through which Russia can create complete havoc in Ukraine; in the Baltic states it can destabilize; co-opt power in Eastern Europe; divide and rule in Western Europe; distract in the US and fan flames in the Middle East and South America.[80] In all the cases, there was an attempt to spread cynicism about participating in elections, create distrust in the electoral process and manipulate public opinion, all of which are key components of the political system of democratic states. Thus, attempting to alter any of these is perceived as an interference in the internal affairs of a state.

[78] US Senate Select Committee on Intelligence, op. cit.
[79] Jens Manuel Krogstad and Mark Hugo Lopez, "Black voter turnout fell in 2016, even as a record number of Americans cast ballots", available at https://www.pewresearch.org/fact-tank/2017/05/12/black-voter-turnout-fell-in-2016-even-as-a-record-number-of-americans-cast-ballots/, accessed on 07 October 2019.
[80] Todd C. Helmus et al., op. cit.

The weaponization of social media by states also aimed to alter institutions of the target state. Safeguarding the institutions of state is one of the crucial components of national security. The institutions of state comprise the entire machinery of government, including its legislative, administrative and judicial bodies and the laws, procedures and norms by which they operate. Since governments largely determine international activity, change in governments can result in significant shifts in their international behaviour and orientation. This often leads the states to interfere in each other's domestic politics.[81] This phenomenon of targeting governments as an institution of state was reflected in the cases presented here. As part of the influence operation in the US, IRA used social media to direct attacks against US institutions including government structure, policies and law enforcement agencies. Analysis of the IRA tactic showed that it attempted to exacerbate discord against the government at federal, state and local levels and there was a clear intention to reinforce tribalism, to polarize and divide and to normalize points of view strategically advantageous to the Russian government on everything from social issues to political candidates.[82]

Regarding political candidates, it was seen that in the 2016 US elections, IRA favoured candidate Donald Trump and disparaged candidate Hilary Clinton. Political candidates and leaders were also targeted in Eastern European countries. In those countries, IRA is believed to have campaigned to influence the political outcomes of the countries in a way to establish a cushion against what it considers malign Western influence.[83] For example, in the 2014 Ukrainian elections, Russia framed the leading candidate Petro Poroshenko as a puppet of the West and campaigned to drive public opinion against him. In Libya, Russian actors promoted two potential presidential candidates who are likely to be favourable to their political interest in the country. In Mozambique, the same actors supported the incumbent president and defamed the opposition. In all these cases a clear pattern of interfering in the domestic politics of a state using social media is visible. But the citizens of a country hold the exclusive right to decide their political preference. Attempts of foreign actors to manipulate this process is a serious challenge to national security.

Foreign actors also targeted the policies of the states as part of its information warfare. For example, IRA intended to achieve policy paralysis in Eastern Europe by creating a wedge between the ethnic Russian or Russian speaking populations and their host government. In Germany, the agency created fissure among the people about the government policy on Syrian refugees. In Turkey, it fears mongered citizens about Turkey joining the EU and in Italy, it promoted the narrative that Italy should leave the EU. In the Middle East, Latin America, the US and UK, Iran used social

[81] Barry Buzan op. cit., pp. 53-57.
[82] Renee DiResta et al., op. cit.
[83] Todd C. Helmus et al., op. cit.

media to push the Iranian political narrative and designed the social media content with an angle that benefited the diplomatic and geostrategic views of the Iranian state. All these were crucial issues during the time these contents were shared. It was a critical political threat for the states as the ideas and institutions attacked by foreign actors were already internally contested. The influence operations exploited the societal fractures and created contents which amplified the existing divisions. Through such operations, an environment of distrust on the state, its policies and institutions were created by a foreign state or a state-backed agency, which is a major threat to national security.

The hostile use of social media also seems to wage attack on the ideology of the states. Russian influence operation in Eastern Europe targeted capitalist economies and Western financial institutions. Through the series of social media activities, it attempted to erode trust on the capitalist ideology among the people in this region. Democracy as an ideology was also attacked in the influence operations. In former Soviet Countries, IRA seemed to have attempted to tarnish the image of democratic leaders and erode trust on democratic institutions through social media content. The National Security Strategy 2017 of the US identified that rival actors of the US used propaganda and other means to try to discredit and undermine the legitimacy of democracies.[84] This showed that both capitalist and democratic ideology were attacked in the information warfare using social media.

It is also perceived that social media-based influence operation challenged the territorial integrity of states to some extent as foreign actors attempted to use the platforms to initiate internal secessionist movements. In the case of Russian interference in the US, it was seen that IRA's social media content targeted American societies to promote territorial split and trigger both secessionist and insurrectionist sentiments like Texas and California exits, i.e., (#texit) and (#calexit). Territorial integrity is a fundamental component of national security and in this case, it seems to be threatened. Besides targeting the state directly, social media-based influence operations were directed to the external interests of states as well. For example, in Turkey, Russia promoted anti-American discourse, anti-US conspiracy theories, undermined Turkey's political and security cooperation with the United States and attempted to create fissures with the West. In Africa, Russia criticized French and American policies. Iran also propagated an anti-West narrative in its target regions. Such activities are major threats to a state's external interests.

While the strategy of the influence operation and its impact on core components of national security are understandable, it is important to assess to what

[84] The White House, *National Security Strategy of the United States of America,* Washington, DC: The White House, 2017.

extent social media advertisements and posts can impact public opinion and affect the decision-making of people. According to Amnesty International's report on the business model of Facebook and Google, the combination of algorithmically-driven ad targeting and personalized content plays an enormous role in shaping people's online experience and determining the information they see. This can influence, shape and modify opinions and thoughts, which risks affecting the ability of people to make autonomous choices.[85] On such platforms, the unique personal characteristics of social media users are used to design and find the best ways to persuade people towards particular outcomes. In the information operations, the state and state-backed agencies took opportunity of this business model, acted like expert digital advertising agencies and used the data-targeting capabilities and persuasion technique of social media platforms to target different groups to influence their decision-making process. In describing the magnitude of the influence capabilities, techno-sociologist Zeynep Tufecki termed these social media platforms as 'persuasion architectures' that can manipulate and influence people at the scale of billions.[86] James Williams, the former Google advertising strategist called it the 'industrialisation of persuasion'.[87] The Council of Europe's Committee of Ministers reported that "fine grained, sub-conscious and personalised levels of algorithmic persuasion may have significant effects on the cognitive autonomy of individuals and their right to form opinions and take independent decisions."[88] This displays that the ads and content used in the influence operations by foreign actors are most likely to have a significant impact on people's decision-making within the target countries.

As the assessment manifests that the weaponization of social media is a growing threat and its impact on decision-making is also evident, it is now important to evaluate whether the issue has been securitized by the state. Securitization is the process in which certain issues within a given political context are both securitized and politicized. It focuses on the existential threat, the security agents and the referent objects.[89] Now if the 2017 US National Security Strategy is analyzed, it can be seen that the document duly recognized the magnitude of information warfare and the use of social media to influence public opinion across the globe. It noted that America's competitors weaponize information by exploiting the marketing techniques to target

[85] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, London, UK: Amnesty International Ltd, 2019.
[86] Zeynep Tufekci, "We're building a dystopia just to make people click on ads", available at https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads?language=en, accessed on 06 December 2019.
[87] Amnesty International, op. cit.
[88] Council of Europe's Committee of Ministers, "Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes", available at https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b, accessed on 15 November 2019.
[89] Leanne Jennifer Smythe, op. cit.

individuals based upon their activities, interests, opinions and values. It defined the Russian influence campaign as a blend of covert intelligence operations, false online personas with state-funded media, third-party intermediaries and paid social media users or 'trolls.'[90] The 2019 Worldwide Threat Assessment of the US Intelligence Community identified cyber espionage, attack and influence as a top global threat.[91] According to the report, China and Russia are becoming more adept at using social media to alter how people think, behave and decide. Iran is also using social media platforms to target US and allied audiences. The document predicted that US's adversaries and strategic competitors are probably already looking at the 2020 US elections as an opportunity to advance their interests and in broader aspect, they almost certainly will use online influence operations to try to weaken democratic institutions, undermine the US alliances and partnerships and shape policy outcomes in the US and elsewhere. There is a growing concern that such attempts would involve deep fakes or similar machine-learning technologies to create a convincing but false image, audio, and video files to augment influence campaigns against the US and its allies and partners. The 2019 policy brief of the European Council on Foreign Relations identified social media manipulation as a hybrid threat. It stated that through social media, disinformation, rumours and manipulation can reach directly into a much wider spectrum of society.[92] Chatham House Report on Cyberspace and the National Security of the United Kingdom identified that the global ICT system can be exploited by a variety of illegitimate users and can even be used as a tool in state-level aggression.[93] This clearly reflects the growing concern among security and intelligence communities regarding the weaponization of social media and efforts to securitize this issue is evident.

By connecting Barry Buzan's analysis of national security threats with the cases assessed here, it can be implied that there is a clear pattern of threats pertaining to state's ideology, social and political institutions, territorial integrity, domestic and foreign policies and external interests due to the weaponization of social media. It denotes a combination of military, political and politically significant social and cultural threats. The threat is also being recognized by the national governments and the international communities and there are increasing efforts to securitize it. This evidently makes the weaponization of social media a major concern for national security.

While the threat has been identified and measures have also been taken to securitize it, at this part it is important to scrutinize the roles and responsibilities of

[90] The White House, *National Security Strategy of the United States of America*, op. cit.
[91] Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, USA: Office of the Director of National Intelligence, 2019.
[92] Gustav Gressel, "Protecting Europe against hybrid threats", available at https://www.ecfr.eu/publications/summary/protecting_europe_against_hybrid_threats, accessed on 18 November 2019.
[93] Paul Cornish et al., op. cit.

the social media companies in tackling such foreign information operations. Owing to the rising pressure, the leading social media companies took multiple initiatives to address the issues but several challenges remain regarding its effectiveness. Twitter has committed to strengthen its efforts against attempted manipulation, including malicious automated accounts and spam.[94] Facebook has taken initiatives to tackle foreign interference, increase transparency and combat misinformation. It also took preventive measures during elections in selected African countries, in Australia, Thailand, India, Indonesia, Mexico, UK and the upcoming 2020 US elections. But the states and state-backed agencies with intent for influence operation are also developing newer and harder to detect ways to conduct their hostile campaign. For example, the use of deep fakes and employment of local citizens as content creators to avoid detection by social media companies are on the rise. Also, the Russian owned social media companies which were key parts of the influence operation in Eastern Europe are beyond such transparency initiatives. These are likely to be used in future influence operations in the region which is a major concern. Also, there is a likelihood that information operation might shift to smaller platforms[95] which raises more concerns regarding its outreach and management. Thus, it can be evaluated that the initiatives of social media companies seem to be inadequate and the actors are choosing alternative platforms and adopting newer and hard to detect methods for weaponizing the platforms. This manifests that the threat of weaponization of social media by the state and state-backed actors is critical and continuously growing.

5. Conclusion

Social media is one of the many wonders of the information age which has become an integral part of our lives. Undoubtedly, it has brought several benefits to almost all spheres of civil and political life. But like most elements of digital technology, it too has turned out to be a double-edged sword. The abuse of these platforms by hostile actors has gradually made it a menace of present time. The same social media features that revolutionized the way we connect to the world have also been used as weapon-grade communication tool. While several actors have used social media for ill intent, the weaponization of social media by the state and state-backed agencies in information warfare and foreign influence operations have threatened the core elements of national security and made it a rapidly evolving national security concern. Through the cases of Russian information warfare in the US, Europe and Africa, and Iran's influence operations in the US, UK, Latin

[94] Twitter, "Elections integrity", available at https://about.twitter.com/en_us/values/elections-integrity.html, accessed on 10 December 2019.
[95] Meg Kelly and Elyse Samuels, "How Russia weaponized social media, got caught and escaped consequences", *Washington Post*, 18 November 2019.

America and the Middle East, the military, political, social and cultural threat on state's ideology, social and political institutions, territorial integrity and external interests are reflected. Even after the debates, discussion and indictment of such actions, the threat persists. Active interference operations are ongoing on several social media platforms and are likely to intensify in the coming days.

The coordinated information warfare campaign of Russia's Internet Research Agency did not stop once it was caught interfering in the 2016 US elections. Engagement rates continued to increase and covered a widening range of public policy issues, national security issues and issues pertinent to younger voters. According to the finding of the US SSCI, in post-Elections Day 2016, Instagram activity increased 238 per cent, Facebook increased 59 per cent, Twitter increased 52 per cent, and YouTube citations went up by 84 per cent.[96] During the testimony of Special Counsel Robert Mueller in front of the US Congress, he warned that not only is Russia attempting political interference right now 'as we sit here', but there are many more countries with similar cyber capabilities that could do the same.[97] Iran has already made significant advancements in such operations and it is continuously evolving. Besides Russia and Iran, there are speculations that more countries are already in the process of adopting this strategy. RAND Corporation's study on Hostile Social Manipulation observed that leading autocratic states have begun to employ information channels for competitive advantage.[98] Although the plans remain in their initial stages, it could unfold in several ways. The report also noted that democracies urgently need to undertake rigorous research on social manipulation to gain a better understanding of its dynamics. It is also required to be incorporated in the cybersecurity strategy. Here it needs to be noted that in the Global Cybersecurity Index 2018, 58 per cent countries reported having a national cybersecurity strategy[99], however, most of these strategies do not adequately address the issue of social media-based influence operations from foreign actors. Also, unlike traditional political advertising, there are rarely any new laws or policies that govern digital political advertising.[100] This calls for the need of more effort in this critical area.

It is alleged that the state and state-backed agencies of Russia and Iran have

[96] US Senate Select Committee on Intelligence, op. cit.
[97] Craig Timberg and Tony Romm, "It's not just the Russians anymore as Iranians and others turn up disinformation efforts ahead of 2020 vote", *The Washington Post*, 26 July 2019.
[98] Michael J. Mazarr, Abigail Casey Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga and James Sladden, *Hostile Social Manipulation: Present Realities and Emerging Trends*, California: RAND Corporation, 2019.
[99] International Telecommunication Union, *Global Cybersecurity Index 2018*, Geneva: International Telecommunication Union (ITU), 2019.
[100] Meg Kelly et al., op. cit.

weaponized social media to conduct information operations which seem to have threatened the national security of the target states. The threat is evolving and there are speculations that more states are likely to adopt to this strategy. Governments have come up with security strategies to address threats regarding cyberspace but most of those do not adequately address the issue of social media based foreign influence operations. Leading social media companies have also taken initiatives to secure their platforms from abuse by foreign actors but the steps are insufficient. The states with hostile intent are finding their ways around those measures. On this basis, it can be concluded that the threats pertaining to the weaponization of social media have sufficiently intensified for the states to address this as a national security concern. As the world is borderless and almost all parts of the world are connected through one or more social media platforms, no states are immune from this evolving threat. This warrants comprehensive actions from government, social media companies, civil society organizations and all relevant stakeholders.