Lahore Institute for Research and Analysis Journal
ISSN: 3007-2700 (Online); 3007-2719 (Print)

Volume 3, 39-53, 2025

From Strategy to Tactics: Conceptualizing Weaponization of Digital Media Platforms across Levels of Warfare

Dr. Zeeshan Zaighum[1], Rana Faizan Ali[2]

[1]*School of Media and Communication Studies, Beconhouse National University, Lahore, Pakistan.*
[2] *School of Media and Communication Studies, Beconhouse National University, Lahore, Pakistan.*

Corresponding Author: [1]zeeshan.zaighum@bnu.edu.pk

Received: 15-11-2024 Revised: 12-01-2025 Accepted: 15-01-2025 Published: 04-02-2025

Suggested Citation: Zeeshan Zaighum; Rana Faizan Ali. "From Strategy to Tactics: Conceptualizing Weaponization of Digital Media Platforms across Levels of Warfare." *Lahore Institute for Research and Analysis Journal* 3 (2025): 39–53.

Abstract - *The exponential proliferation of digital media platforms has reshaped the nature and character of modern warfare, establishing novel challenges in the Information Environment. The weaponization of social media platforms have intensified the 'fog of war' as the very concept of it lacks clarity. This paper conceptualizes the weaponization of digital media platforms at four levels of warfare: strategic, operational, tactical, and intelligence. The paper is based on existing literature and case studies. At the strategic level, digital media is used by adversaries to create offensive narratives with long-term strategic objectives. Whereas adversaries use digital media platforms to carry out targeted 'Influence Operations' to achieve cognitive objectives. This is manifested in the social and psychological fragmentation of society. At the tactical level, digital media trends and tactics help proliferate real-time PsyOps (psychological operations). This is done by deploying bots, trolls, and creating trends to permeate disinformation against state and state actors in an information environment. While at intelligence level, the paper poses various techniques of intelligence collection in the domain of SOCMNIT (Social Media Intelligence). The paper offers insights into the complex interplay between the fragility of the information environment on digital media and cognitive vulnerabilities in the context of contemporary warfare. The four-layered framework provides a conceptual foundation for policymakers and strategists to address the pervasive weaponization of digital media platforms in contemporary fifth-generation warfare.*

Keywords - Information Warfare, Digital Media, Social Media Intelligence, Strategic Communication, Cognitive Security

1.Introduction

The rise of strategic communication has changed the way information warfare is planned and executed. Information warfare is not mainly focused on information but it is now more focused on the effects that a piece of information has created.[1] In many cases, information is the only

[1] Z Zaighum and F Rasool "Mapping Fault lines in the context of Hybrid Warfare: A Case Study of Pakistan.

difference between and among effects. In past, information and its effects were limited by technologies and rigid knowledge system of a society. Therefore, propagandists would struggle to infuse a new ideology in an information environment. Territorial boundaries were also reflected in media systems. State ideologies and media organizations would complement and support each other. With the emergence of social media, territorial boundaries are now meticulously blurred.[2] Digital virtual public sphere has over encompassed rigid traditional media organizations. Social media platforms now provide sensory knowledge (through technological determinism), group experiences, and scientific evidence for knowledge and information creation.

In a technologically mediated world, users are readily persuaded to accept newer information and ideas. Boyd presented the OODA (Observe, Orient, Decide, Act) loop. OODA loop describes that a person first observes the situation.[3] The observation of situation means factuality and plausibility of the elements in a situation. After this, the person orients her/himself. Orientation means when a person aligns. Then the person decides. The decision-making process is influenced by a person's observation of the situation and his/her orientation in the situation. Eventually, the person acts.

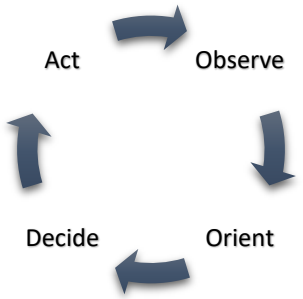

Figure 1: OODA Loop by Boyd (2018)

However, otherwise simple looking OODA Loop becomes very complex on social and digital media platforms. With excessive information, real and fake news, intimidation, coercion, propaganda, disinformation etc., it has become difficult for OODA loop to be fully matured.

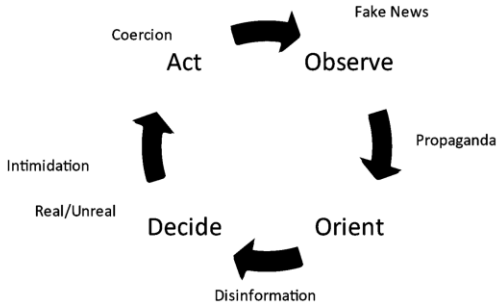

Figure 2: OODA Loop and Social Media-Proposed by the researchers

OODA Loop becomes a complex phenomenon where confusion is prevalent in users' minds. The

International Review of Social Sciences, 2021.

[2] A Chaudhary, Z Zaighum, and F Ali, (Information Warfare and Twitter: A Nexus of Indian Shadow Networks on Balochistan Issue. NDU Journal, 2024).

[3] Danah Boyd, "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications," in *A Networked Self* (Routledge, 2010), 47–66.

weakening of OODA Loop in warfare has remained a key area of focus for campaigners. In fourth and fifth generation warfare, the model is used to debase informed opinion formation by a society and becoming vulnerable for exogenous influences.

1.1 Fragility and Vulnerability of Beliefs

According to Boyd, OODA loop is biologically and socially determined. Social constructs including race, ethnicity, nationality, gender, religion, political ideology, and biological constructs like sex, genes play an important role in the loop.[4] Social media has made social constructs to be dynamic. With newer meaning and novel interpretation of constructs, and exposure to new but technologically mediated experiences- knowledge creation and acceptance, and beliefs formation and sharing have become vulnerable. Knowledge is the base of our action. If knowledge is controlled, actions can be controlled as well.

Traditionally, targeting knowledge system of a large group of population was difficult. As populations were widely spread, belief systems were individualized, and mass media was limited in reach. However, social media and internet has concentrated large number of individuals and wise spread population one virtual public sphere where physical and ideological differences have become significantly extraneous. Szafranski argues that targeting a large number of populations through technology would become easier. Knowledge system would become fragile and ideologies vulnerable. Attacking population and leadership would be possible. Knowledge and beliefs system depend profoundly on the strengths of narratives. As discussed above, contemporary information warfare is not mainly focused on information but on the effects and meaning of information. Meaning is a take away for any consumer. Actions are determined by the very meaning of piece of information. Narratives give meaning to the audience. Narrative become relevant in a fragile information environment.[5]

1.2 Narratives and Cognitive Security

There is no war in the world without narratives. There is no group in the world without its narrative. Narrative identity theory poses that individual tell stories of events, persons, and groups to make narratives. These narratives provide them identity. However, narratives are not just concerned with identity only. Narratives are important and relevant in cognitive security both individually and collectively. Cognitive security in the integrity of human cognition. Fragility of beliefs and opinions indicate low cognitive security.[6] Narratives are the building blocks of cognitive security. If narratives are powerful, cognition remains intact and secure from any internal or external manipulation, if narratives are weak, human cognition can easily be swayed.[7] Furthermore, narratives and cognitive security can further be explained in a multidimensional context. Firstly, cognition is the process of acquiring information through experience and observation. The role of perception and frame analysis is crucial here. Social narratives provide barometer for perception and frame analysis. If social narratives are strategically created and remain intact, collective and social cognition becomes impregnable to any manipulation. Secondly, narratives and institutional trust are also related. In a country, it is important that general population keeps its faith and trust in institutions. Narratives are constituents of public trust in social, political, and state institutions.

---

[4] Chet Richards, "Boyd's OODA Loop," *Necesse* 5, no. 1 (2020): 142–65.

[5] Szafranski, *Theory of Information Warfare: Preparing for 2020*.

[6] Imran, L Zaighum, Z Ali RF "Military-Public Relations: A Study of Contemporary Information Warfare in Clausewitz Trinity through CogSec Perspective Laiba Imran* Dr. Zeeshan Zaighum Rana Faizan Ali," *Lahore Institute for Research and Analysis Journal* 1 (2024): 39–52, https://journal.lira.pk/LIRA/article/view/18.

[7] Szafranski, *Theory of Information Warfare: Preparing for 2020*.

Thirdly, in order to maintain law and order- public's trust in institutions must remain secure. Narratives provide all three dimensions.[8] Studies of Almang[9] and Korypko[10] reveal that adversaries, enemy states, and hostile intelligence agencies (HIA) become successful when governments and countries start losing war of narratives. Color Revolutions become successful when people start losing faith in their governments.

Corman argues that the project had millions of dollars funding. Project covered results subjects from Christianity, Hinduism and Islam. Quantitative research methods and neuroscience was used to comprehend results.[11]

1.3 DARPA: KAIROS

Weber et al. argue that DARPA developed "Knowledge-directed Artificial Intelligence based Reasoning Over Schemas (KAIROS)" to make sense and meaning out of complex world issues.[12] The purpose of the program is very obvious. Any event in the world may have a bearing on diplomacy, economy, national security, and defense. With convergence of technologies and world becoming a global village- transnational communication has challenged human capacity to comprehend ever changing global horizon. Therefore, DARPA planned to design a semi-automated program. The program was based on artificial intelligence to store and develop human schemas to better understand public reactions in different scenarios.

The system has been designed in two stages. In the first stage, system collects information from big data sources, multi-media content, and human input. In the second stage, the findings are applied to information created in different languages and multiple technologies to excerpt understanding from complex issues So far sixty events have been run and identified in KAIROS.

1.4 Narratives- What are they?

Narratives are not facts. Narratives are interpretations of complex stories, incidents, events, or issues. Narratives are mechanism to derive meaning and create sense. Without a narrative nothing would have a meaning or interpretation. Narratives provide individuals an identity to live, a meaning to survive, a reason to thrive. Narratives are not subjective or objective.[13]

There is no parameter to validity the neutrality of a narrative. For neutrality is not to be associated with a narrative. The structure, composition and use of narratives is strategic. There is no example where narratives lack strategy. As mentioned earlier, narratives are not facts but interpretation. The interpretation is not limited to events and stories. Narratives give interpretation of actions, individuals, characters, movements, and groups with the person to give "meaning" through "identification."[14] Narratives are not isolated and scattered stories with no integration. Narratives are widespread stories merged into one comprehensive interpretation.

However, Nissen presents a more specific approach to look at narratives, and argues that narratives

---

[8] T E Nissen, *#TheWeaponizationofSocialMedia @Characteristics_of-Contemporary-Conflicts* (Copenhagen: Royal Danish Defence College, 2015).

[9] J Almang, *War, Vagueness, and Hybridwar* (Routledge, 2019).

[10] A Korypko, *Hybrid Wars: The Indirect Adaptive Approach to Regime Change* (Moscow: People's Friendship University of Russia, 2015).

[11] S Corman, *Narrative Networks (N2) Phase I Progress, Status and Management Report* (Tempe: Arizona State University, 2013).

[12] N Weber et al., Human scheme curation via casual association rule mining. 2021.

[13] A Maan and P Cobaugh, *Introduction to Narrative Warfare: A Primer and Study Guide* South Carolina : CreateSpace Independent Publishing Platform, 2018.

[14] Maan and Cobaugh.

are created by state and political actors of the country.[15] Therefore, state narratives are political savvy and thereby, political created. Narratives are non-linear; therefore, they have no beginning and no end. Moreover, in order to keep information intact, an information environment must be kept saturated with favorable narratives. Maan categorizes narratives into the following:

2. Narratives

This category is simple and easy version of events, incidents, actions, and characters. Such narratives do not require any opposing narrative or a group.

2.1 Counter-Narratives

Counter narratives are alternative and opposite rendering of events, actions, incidents, and characters. Although, counter-narratives are opposite to an existing narrative, but counter-narrative may not necessarily engage an adversary through starting a narrative war. Counter-narratives must be compatible with existing narratives in terms of the use of facts and stats. Counter-narratives must recontextualize established meanings previously used stories and incidents.

2.2 Offensive Narratives

Offensive narratives are one of the most practiced tools of contemporary narrative warfare and are strategic in nature but they are also used operationally and tactically. Offensive narratives directly attack and engage an adversary in a narrative war.

2.3 Defensive Narratives

Defense narratives are not choice but necessity. Defensive narratives become inevitable after offensive narratives. The scope and threshold of defensive narratives remain questionable in the comparison with offensive narratives.

2.4 Structure of Narratives

The structure of narratives is simple. Similar to any story, a narrative has a starting point, a mid-point and an end.

Maan and Cobaugh dissect the structure of narrative into the following:

2.4.1 Meaning

Different people may interpret one message differently. The interpretation of message is based on existing schemas of a receiver. Therefore, meaning is associated to characters, actions, ideologies, events, and incidents. Meaning plays a significant role in developing collective schemas of a group/society. Meaning may not necessarily be based on facts or true.

2.4.2 Identity

Meaning remains incomplete without identification. Identification can be based on socio-cultural-political-religious binaries. An identity itself may not necessarily be common for all groups in a country. But they may definitely share same or similar layers of identity. In a globalized world, identity has become more relevant than ever before. Every group, institution, political party, leader, government, and state thrive for unique, favorable identity. State and non-state

2.4.3 Content

Content is central to any narrative. Meaning and identity are intangible part of narrative but content is the tangible elements of narrative. Images, facts, alternative facts, information, misinformation, reports, rankings, ratings, disinformation, malinformation, speeches, actions, quotations, events, news, paintings, monuments, buildings, graphics, animation, news clippings, footages whether real or doctored are included in the content. Content strengthens meaning and identity of narratives.

2.4.4. Structure

Structure is simply the composition of message. How the meaning is associated? What content is

[15] Nissen, *#TheWeaponizationofSocialMedia @Characteristics_of-Contemporary-Conflicts*.

used? Which identity is included? structure answers all these questions. Structure is simple but not trivial. The structure of narrative plays a decisive role in the effectiveness of a narrative.

3. Media and Cross-Media Narratives

Maan Cobaugh argues that narratives are not natural and raw existence. They are well thought and properly planned. In the contemporary world, owing to the omni presence of information and communication technologies, information is created at an infinite level. This information is used by individuals to form opinions. All countries, states, governments, institutions, political parties, religious groups, non-state actors, media houses, corporate groups, civil society work intensely on narrative building and creation. Any campaign of narrative building has one key aim- to influence behavior desirably. Target audience of the behavior change can be internal/local population or external/foreign population.

Nissen stresses the importance of narrative creation and dissemination across all media platforms. Moreover, narrative building requires comprehensive data sets. Narratives are more effective if they are compatible with existing beliefs and biases. Individuals prefer information that matches their existing knowledge. Individuals consciously and sub-consciously reject information that challenges their knowledge and beliefs. Therefore, content must be aligned with public's acceptability of information.

Furthermore, people use media and communication channels for different purposes. In addition to this, different channels have varying reach, penetration, and effectiveness. Even internet is not one channel. As discussed earlier, IDF used different social media platforms for different purposes. Internet, digital, and social media platforms can be divided into several categories. Firstly, there are webpages which are accessed on mobile phones and computers through browsers. Then, there are social networking websites including Facebook, Twitter, etc. There are video sharing websites like YouTube. Besides this, there are messaging apps like WhatsApp. Then, there are collaborative projects like Wikipedia.

Narratives cannot be disseminated in singularity of one media platform. Narratives must be created and spread across all media channels platforms. Therefore, multiple media platforms are selected for a campaign. Following are the approaches which are used to spread narratives on across media platforms[16]

3.1 Push

This includes dissemination of content on all selected platforms. In this approach, content largely remains the same, only few changes are made.

3.2 Extra

In this approach, some additional information is also added along with the main content. This approach is widely used in Twitter and Facebook.

3.3 Structure

The structure of the content is planned in a way that motivates readers to move to main platform. Hyperlinks, clickbait are few practices to be added into the structure.

3.4 Hands-off

This approach motivates and encourages common users to create content of their own, modify an existing content, or support it. This narrative building approach is non-linear.

Miller presents four conditions for any narrative building campaign to be "cross media". Firstly, the project must not be restricted to one platform. Secondly, it must not be completely static or non-reciprocal. Target audience must be engaged through interactivity. Thirdly, main messaged

[16] Nissen.

must be supported by additional and extra information. Fourthly, additional information must be compatible with main message.[17]

4. Weaponization of Digital Media: Operational Level

Social media platforms have been weaponized at the operational level as well. Traditionally, social media was used for cliched Information Operations (IOs). However, latest trends and widespread use of social media in warfare has transformed the use of social media in more holistic Operational domain. One such case is designed and proposed by Nissen. The holistic weaponization model called "Effects Based Thinking". The model explains "effect" as to be an outcome in form of a behavioral or a systematic change. The model six interlinked operations which are both linear and non-linear. The operations are discussed in the following:

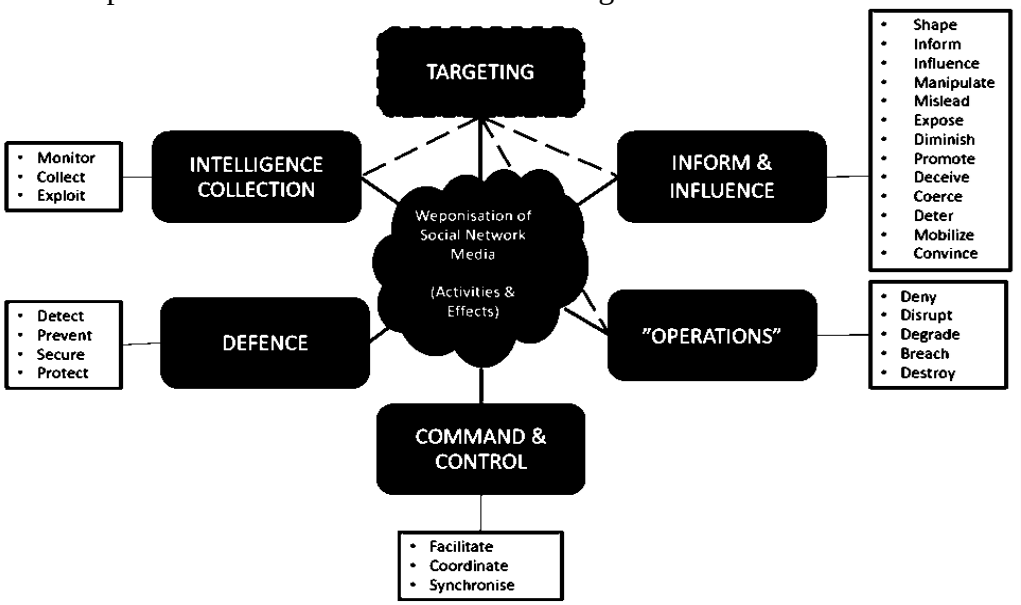

Figure3:WSM Activities by (Nissen, 2015)

4.1 Targeting

It is an act of identifying and extract target audience from a pool of varying groups. Digital media consists of hundreds and even thousands of social groups and bubbles. However, not all groups or individual are equally relevant to a campaign. Therefore, identifying and targeting groups which can generate better results and produce desired effects are targeted on social media platforms.

Targeting is also a well-organized activity. In the process, focus is not restricted to one platform but all platforms are used and observed, activities and events are also coordinated.

Only individuals and groups are not targeted on or through social media platforms. Narratives, news, information, opinions, systems, networks on interest are also identified as potential targets.

4.2 Inform & Influence

Inform is to spread the desired information. Influence is the ability to have an outcome on thinking or behavior of an individual. Both are combined for better results. The purpose is to rout a change in thoughts and actions both individually and collectively. For this purpose, facts and alternative facts, truth and post-truth are used and manipulated in communication to leave a colossal damage to target's rational thinking. This manipulation can trigger misled actions by target audience/entity.

[17] C H Miller, *Digital {Storytelling}: {A} Creator's Guide to Interactive Entertainment* (Amsterdam: Elsvier, 2008).

In order to mislead target, both “diminish” and “expose” techniques are used. An information can be detrimental to public thinking if exposed. And similar information can cause false perception if diminished. Influence is also achieved through coercion and intimidation. Specially, terrorists’ organization use intimidation and coercion to influence. Mobilizing and convincing a target population to take an action is also included in this category. Color Revolutions are good examples of mobilizing to take an action.

4.3 Operations

Social media operations are not restricted to targeting human cognition. Operations also include attacking communication networks, systems, data bases, and platforms. There are several techniques of such approaches. The first technique is to “Deny”. This technique is used to deny any communication or service to a target population. This technique is used by both state and non-state actors. This technique was also used in “Operation Armageddon”. The second technique is to “disrupt”. This technique is used in attacks which are planned to temporarily or permanently destroy a service, system, or data base. Third technique is to “degrade”. This technique is used to malign or to smear an existing system, service, or platform. This is usually done by hacking. Other ways include creating imposter accounts, fake/doctored content. Fourth technique is to “breach”. This technique is used to infiltrate into an information system or database with an objective to extract information or destroy it. Fifth technique is to “destroy” an information system, service or database. All these five techniques are not sequential but interlinked.

4.4 Command & Control

“Command and Control” activities and operations of social media weaponization are tripartite. The actions include to “facilitate”, “coordinate”, and “synchronize”. The command and control of social media operations are not usually established in campaigner’s homeland. These are established either in target population’s country or in a foreign land to avoid attribution.

4.5 Defence

Defence is another activity of social media weaponization. Defence includes detecting a threat. In traditional warfare, kinetic attacks were easy to detect. However, in modern communication warfare, especially in information and cognitive domain detection of an attack is very challenging. Information Operations are planned and executed in an internalized and localized manner. Thereby, detection becomes difficult. Nevertheless, detection remains the first layer of defence. The second layer of defence is to protect. Those who are exposed to an attack must be protected. Third layer is prevention. Prevention is to avert potential targets from attack. The last layer is to secure that includes creating a safe parameter from current or future attacks.

4.6 Intelligence Collection

Intelligence collection is the last activity of EBT model. Intelligence collection involves monitoring, collection, and exploitation. Intelligence is an offshoot of several activities including gathering and organization information. It also includes establishing and using evaluation parameters for extracting analysis from information. The information of interest can be related to any individual, groups of individuals, geographic area, institution, system or even database. Any information of interest related to Online and offline information environment is collected. Intelligence on social media platforms is slightly different from traditional information environment. On social media platforms, information often pertains to user behavior, sentiments, opinions, networks, and groups.

5. Theorizing weaponization of digital media: Tactical Level

At the tactical level, social media is used for several purposes. Social media tactics are integrated

with holistic Information Operations to achieve better results. One of the tactics used in Information Operations includes projection of terrorists' activities on social media platforms to help spread fear. For instance, ISIS created thousands of social media accounts to promote and glorify its activities[18] IDF created "Hashtag trends" during "Operation Cast Lead", "Operation Pillar of Defence", and "Operation Protective Edge"[19]

Social media platforms support and amplify spread of narratives from one group to another. A narrative is ether created or initially accepted by a group of hard/true believers of the narrative or the campaigner. In order for narrative to be fully spread from one cluster to another, it must be suitable with an existing narrative or a cultural narrative of the past. A narrative must have a group of ideologues who possesses desirable cognitive biases towards the narrative, and accept any information with preconceived credibility. This spread can be catalyzed with the help of cyber operators and cyber warriors[20] These cyber warriors and bots create hashtag trends. These hashtags are fed with both system-generated and user-generates content. Use of disinformation, fake news, doctored images, hate speech, trolls, flamebait facilitate campaigners to achieve operational goals tactically.

5. Hashtag Trends

Hashtag trends are widely used in Information Operations. Lt. Col. Jarred Prier of the US Airforce has presented three types of operations related to hashtag trends which are discussed in the following[21]

5.1 Trend Creation

The most widely practiced IO related to hashtag trend is "trend creation". Trend creation requires ample monitory, human, and systematic resources. Trend creation is a preferred IO because it allows for penetration and access to an online Information Environment. Trending hashtags are reflection of public sphere and public discourse. Creating a hashtag and making it trending are two different chores. A hashtag may be created by a real or a fake account and can also grow organically. But this does not guarantee that the hashtag will trend. Therefore, pools of bot accounts are used to grow a hashtag into 'trending'.

5.2 Trend Hijacking

Any online information environment is always saturated with trending hashtags at any given time. "Trend Hijacking" as the name suggests, involves taking control of hashtag that is already in trending. A hashtag is not a property or ownership of one account. A trend is a public proprietary. Hijacking a trend requires less human and monitory resources. Taking control of a trending hashtag is simply done through bot accounts. These automated and system operated accounts are used to 'push' content into a trend. Massive creation and dissemination of content derails public discourse towards a desired direction.

5.3 Trend Distribution

Polluting an online Information is another type of IOs on social media. This activity includes posting and commenting propaganda and disinformation messages on all trending hashtags. It is not important and relevant that trending hashtags are related to messages or not. This activity is carried out through bot activity and artificial accounts.

---

[18] A Maan, *Narrative Warfare* (South Carolina: {CreateSpace} Independent Publishing Platform, 2018).

[19] D L Liang, *Battlefront New Media Lessons For The {SAF} Based On A Study Of The Information Campaign During Operation Pillar Of Defence* (Journal of the Singapore Armed Forces, 2015).

[20] J Prier, *Commanding the Trend: Social Media as Information Warfare* (Strategic Studies Quarterly, 2017).

[21] Prier.

5.4 Trolling

Trolling is an act of ridiculing some individual, group, institution, or even a country. Trolling is not new information warfare. Conventionally, "flamebait" are used to provoke an action. Flamebait is a question whose answer reveal aggressive differences among members of a group. Flamebait is widely practiced on social media platforms. Users follow social media groups, discussion forums, pages, blogs etc. Trolls pose questions which generate long discussion threads. These discussions are usually heated and fiery in nature. These discussions are called 'flamewar'. The effects of such discussion may also be converted into physical world in form of hate related crime and at times, extremism. Trolls and bot accounts are used to carry out flamebait.

However, trolling is not limited to flamebait only. Memes can also be categorized into act of trolling. Memes by nature, are funny and witty. Users usually take memes lightly. However, memes are widely used in political communication and as well as information warfare. During Operation Protective Edge and Operation Pillar of Defence of the IDF, memes were extensively used to ridicule adversaries. Following are the patterns of Trolling as Identified by NATO's Strategic Communication Centre for Excellence.[22]

5.4.1 Aggression against other participants

The very purpose of trolling is to provoke a person to react. A troll usually uses offensive slurs and abuses to aggravate response. A troll may also opt for personal attacks and even vulgarism.

5.4.2 Labeling

The politics of naming and labelling is a pattern of trolling. Labelling includes association or naming with terrorist groups, traitors, non-state actors, criminals, separatists, foreigners, theophobic and xenophobic expressions.

5.4.3 Use of historical references

In order to instigate an animated reaction, a troll may also use historical references. Widely accepted traitors, criminals, villains of modern and ancient history are used for association.

5.4.4 Demonstrating civilization or moral superiority

Trolling is humiliating and chastening an individual or a group. By indicating own cultural, religious, political, professional, national, racial or institutional superiority, a troll tends to ridicule a target. Furthermore, demonstrating higher moral and ethical superiority, displaying self-righteousness also insinuate humiliation for others.

5.4.5 Use of irony and sarcasm

A troll also uses witty and sarcastic comments to scorn. A troll mocks leaders, followers, individuals and groups to incite anger and gain response.

5.4.6 Conspiracy Theories

In order to sow confusion, trolls may disseminate conspiracy theories as people are often skeptical of events that appear straightforward. Therefore, owing to novel and attractive nature of conspiracy theories, made events and stories spread easily.

5.4.7 Diverting Discourse

Trolling is also used to divert public discourse from one topic to another. It is widely observed that trolls, through the mentioned patterns divert attention.

5.4.8 Social Proof

Among many, one of the purposes of Information tactics is to support an action. Social proofing is an attempt to normalize an abnormality in the society. Trolls are used to social proof anomalies by presenting a social pattern.

---

[22] NATO., (Kalnciema iela: NATO, 2016).

5.4.9 Dehumanization

Trolling includes spreading hate through humiliation. A troll may tactically dehumanize targets.

5.4.10 Data Attacks

Trolls are also designed as 'Talking Bots'. Trolls are used to spread fake news and false information. Trolls bombard conversations and discussions with unverified and exaggerated attacks.

Traditionally, trolls are defined as individuals who instigate conflict and incite heated discussions. It is evident that trolls enjoy attention given to them by users in a discussion thread. Trolls also relish excitement of conflict and drama. Trolls are usually sadist by nature and consequently, trolls use disruptive, destructive, derogatory, and deceptive tone and content to offend targets. Aforementioned points may well suit for individuals. Human trolls have certain limitations. Humans cannot exceed the time barrier, nor can they simultaneously share content across hundreds of accounts. An individual cannot create and post content at a very large scale. Nevertheless, trolls are not always individuals or humans. Trolls can be automated and computer operated bots who can serve the purpose of trolling. Hybrid trolls are operated in groups. Command and control center of trolls is called trolling farm or trolling factory.

5. Weaponization of digital media: Intelligence Level

Intelligence is monitoring, collection, and exploitation of information. Intelligence is an offshoot of several activities including gathering and organization of information. It also includes establishing and using evaluation perimeters for extracting analysis from information. The information of interest can be related to any individual, groups of individuals, geographic area, institution, system or even database. Any information of interest related to Online and offline information environment is collected. Intelligence on social media platforms is slightly different from traditional information environment. Traditionally Intelligence is divided into three activities.[23]

5.1 Monitor

Monitoring is the basic purpose of social media intelligence. Keeping a systematic surveillance on public discourse, content, networks, and locations. Monitoring includes tracking information systems, databases, data trends, and attacks/potential attacks. Social media warfare has traces in mosaic warfare. Social media groups and forums are widely spread across online information environment. Unlike offline information environment, social media do not have territorial boundaries. In defence studies, having a defined perimeter makes defence easy. While in the absence of these territorial boundaries on the social media, defence is an Achilles heel. Ergo, monitoring becomes core aspect of protecting online information environment.[24]

Social media monitoring is real time and as well as time displaced. All hashtags which are in trending can be analyzed in real time and can also be evaluated later on. Similar is the case with content. All public discourse encompassing from videos to images, texts to audio, memes or trolls-everything can be (or is) monitored and evaluated. Monitoring is also at different levels. Micro level monitoring is having surveillance on individual accounts, groups, pages, forums and even platforms. Macro-level monitoring is having surveillance on public discourse, discussions, trends and opinions.

---

[23] NATO.; Nissen, *#TheWeaponizationofSocialMedia @Characteristics_of-Contemporary-Conflicts*.

[24] Nissen, *#TheWeaponizationofSocialMedia @Characteristics_of-Contemporary-Conflicts*; NATO., 2016.

5.2 Collect

The second activity is collecting information. Any IO is based on information. Social media platforms are compositions of infinite number of information and data. Extracting relevant and important information is one of the key areas of this activity. Collection of information is determined by the nature of IO. For instance, if IO is an offensive one, potential target, operation theatre, vulnerable groups, integration of IRCs must be done. All the aforementioned activities would require specialized and specific intelligence. Similarly, if IO is based on monitoring, 'who is doing what?' needs to be answered. If IO is related to color revolution, core, vanguard, cohort, and sympathizers of the movement need to be identified; geo-location and network analysis would be required.

5.3 Exploit

The third activity is to 'exploit'. In this activity, a solicited campaign is designed by a Hostile Intelligence Agency (HIA) to exploit cognitive vulnerabilities of TA. Exploitation can be achieved on the basis of the first two activities. Unlike offline IE, online IE is accessible by anyone from everywhere. HIAs working to capitalize fault lines in IE collect and disseminate information that can have detrimental effect on collective thinking.

During intelligence collection monitoring and collection of information is usually done in an integrated manner. Following are some of the analyses which are conducted in intelligence collection.

5.4 Target Audience Analysis

Target Audience Analysis (TAA) is an analysis conducted prior to the planning and designing of IO. TAA helps in identifying most vulnerable groups from pools of population. Depending upon the nature and scope of IO, TAA helps in designing tailored content for better efficacy. People are divided into social sets. Each social set has its own hierarchy, norms, ethos and 'issues'. In one social set, members share knowledge, experiences, biases, and opinions. These social sets may expand through social media discussions and exposure to the content. Nevertheless, in offline world, proximity among users remain most relevant. Therefore, TAA helps in identifying the most relevant and vulnerable groups as targets.[25]

5.5 Factor Analysis

Human Factor Analysis (HFA) is similar to TAA. However, in HFA the main objective is to identify those factors which are influential in determining human perception and as well as actions. Similar individuals may behave differently in one situation. In one society, different individuals may have different experiential knowledge. Same age group may have varied spatial resonance. Factors which are analyzed in this analysis include demographic factors and psychographic factors. Demographic factors include but not limited to age, gender, ethnicity, race, city/state, country, education, occupation, income etc. Psychographic factors may include trauma, distress, political affiliation, religious ideologies, sectarian beliefs, frame analysis, perceptions, opinions, attitudes, receptibility etc. HFA helps in identifying the most effective psychological and demographic factors which can support an IO.[26]

5.6 Social Network Analysis

Social Network Analysis (SNA) is traditionally termed as 'Network Analysis'. SNA can be conducted both in real world and as well as on social media platforms. SNA helps in

[25] Nissen, *#TheWeaponizationofSocialMedia @Characteristics_of-Contemporary-Conflicts*.
[26] Nissen.

comprehending complex social structures either created physically or virtually.[27] Humans by nature prefer to remain in proximity of like-minded people. Social media groups exemplify homophily, where individuals gravitate toward like-minded peers. Social media algorithms function in a way which strengthen and support preferred content and like-minded people.

However, it can be difficult to fully expose a network of the like-minded people on social media. In case of terrorist and extremist organizations, non-state actors, militias, estranged and separatist groups- it is difficult to identify social networks. One technique that has been proposed by RAND is to identify "Seed Account" (SA). "Seed Account" is a level zero investigation. SAs usually belong to prominent leaders, members or officials of a group. People in their networks, connected to them through social media platforms; speaking in their support on television or on social media- their accounts are in level 2 investigation. Users connected or related to level 2 accounts are studied in level 3. And this way, three levels of investigation is done to conduct SNA.[28]

5.7 Geo-Analysis

One of the challenging features of social media for intelligence is collection is extracting the location of the accounts particularly those who are in involved in anti-state or anti-social behavior. Fake accounts, imposter accounts, bots, identity theft accounts and paid accounts are commonly created and operated. These accounts are crucial in conducting IOs by HIA. The locations from where these accounts are operated are hard to trace as servers of global social media service providers are placed all around the world. State agencies and governments do not have direct access to these servers and databases and therefore, they rely on other sources to extract such information. There are two ways of conducting Geo-Analysis: "Geolocation" and "Geo-inferencing". Geolocation is an easy but rarely effective technique. Most of the social media users switch off GPS feature on their devices while using internet and therefore, geolocation does not usually generate large scale success. On the other hand, geo-inferencing relies on metadata. Any piece of information that is posted, shared, forwarded or even downloaded has inherently metadata. The metadata includes digital foot print, device's and user's information. Metadata can be extracted through universally available tools.[29]

5.8 Behavioral Analysis

Analyzing behavior and actions of individuals and groups are fundamental in intelligence collection. Big data trends are monitored and observed all over the world. There have several projects for intelligence collection where programs were designed to analyze social media behavior of individuals and even countries. Sentient World Simulations (SWS), KAIROS, Narrative Networks are projects of DARPA for the US Department of Defence designed to study individual and collective behavior of social media and internet users.[30] IOs are designed on the projections and findings of behavior analysis.

5.9 Trend Analysis

Trend analysis is based on trends which have been discussed in the section "weaponization of social media: operational level".

---

[27] W Marcellino et al., *Monitoring Social Media- Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations* (Santa Monica: RAND, 2017).

[28] Marcellino et al.

[29] NATO., *(2016).*

[30] Weber et al., *(2021)*; T Cerri and A Chaturvedi, *Sentient World Simulations ({SWS}): A Continously Running Model of the Real World* (West Lafayette : Purdue University, 2006); Corman, *Narrative Networks (N2) Phase I Progress, Status and Management Report*.

5.10 Other Methods

Other methods include Content Analysis, Sentiment Analysis, and Discourse Analysis. Content Analysis includes analyzing content that is posted on the social media and internet platforms. The unit of analysis include videos, footages, images, memes, text, animations, audio, posters, messages, news stories etc. The purpose of content analysis is to extract themes from the data. Sentiment Analysis on the other hand focuses on analyzing sentiments posted or reflected in the content people share. The nature and categorization of the sentiment is conducted in this analysis. Whereas, discourse analysis comprehends public discourse, used language, words, expressions, meanings and insinuations.[31]

6. Conclusion

The contemporary communication technologies also help in collecting information regarding an adversary. In warfare, understanding an adversary's strengths, weaknesses, and strategies has always required significant effort and strategic deliberation. Moreover, the importance of such information is widely accepted as such information can play a decisive role in a battlefield. Internet and social media is given significant importance in threat perception by the state. Owing to free and easily accessed of social media, non-state actors, violent non-state actors, terrorists also social media platforms. Studies of explain how terrorists groups like ISIS used social media platforms for only radicalization but also recruitment and spread terrorism internationally, Owing to complex interplay of social media algorithms, manipulation of facts, bot accounts and astroturfing, lower digital media literacy has resulted into social media and social media users as to be in highly vulnerable place. As first hand response strategy. However, it is important for the state to ensure teaching digital media literacy for citizens specially youth. It is also important that the state adopts a whole of government and whole of nation strategy to respond to fifth-generation threats against the country. Inclusion of marginalized groups, under developed communities, dissenting opinions in the national framework would not help guaranteeing national integration but will also help in wiping numerous fault lines from the country.

References

Almang, J. *War, Vagueness, and Hybridwar*. Routledge, 2019.

Boyd, Danah. "Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications." In *A Networked Self*, 47–66. Routledge, 2010.

Cerri, T, and A Chaturvedi. *Sentient World Simulations (SWS): A Continously Running Model of the Real World*. West Lafayette : Purdue University, 2006.

Chaudhary, A, Z Zaighum, and F Ali. Information Warfare and Twitter: A Nexus of Indian Shadow Networks on Balochistan Issue. {NDU} Journal, 2024.

Corman, S. *Narrative Networks (N2) Phase I Progress, Status and Management Report*. Tempe: Arizona State University, 2013.

Imran, Laiba, Zaighum, Zeeshan and Ali Rana Faizan. "Military-Public Relations: A Study of Contemporary Information Warfare in Clausewitz Trinity through CogSec Perspective. *Lahore Institute for Research and Analysis Journal* 1 (2023): 39–52. https://journal.lira.pk/LIRA/article/view/18.

Korypko, A. *Hybrid Wars: The Indirect Adaptive Approach to Regime Change*. Moscow: People's Friendship University of Russia, 2015.

Liang, D L. *Battlefront New Media Lessons For The SAF Based On A Study Of The Information Campaign During Operation Pillar Of Defence*. JOURNAL {OF} {THE} {SINGAPORE} {ARMED} {FORCES}, 2015.

[31] Marcellino et al., *Monitoring Social Media- Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*.

Maan, A. *Narrative Warfare*. South Carolina: {CreateSpace} Independent Publishing Platform, 2018.
Maan, A, and P Cobaugh. *Introduction to Narrative Warfare: A Primer and Study Guide*. South Carolina : {CreateSpace} Independent Publishing Platform, 2018.
Marcellino, W, M L Smith, C Paul, and L Skrabala. *Monitoring Social Media- Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. Santa Monica: RAND, 2017.
Miller, C H. *Digital Storytelling: A Creator's Guide to Interactive Entertainment*. Amsterdam: Elsvier, 2008.
NATO. Kalnciema iela: NATO, 2016.
Nissen, T E. *#TheWeaponizationofSocialMedia @Characteristics_of-Contemporary-Conflicts*. Copenhagen: Royal Danish Defence College, 2015.
Prier, J. *Commanding the Trend: Social Media as Information Warfare*. Strategic Studies Quarterly, 2017.
Richards, Chet. "Boyd ' s OODA Loop." *Necesse* 5, no. 1 (2020): 142–65.
Szafranski, C R. *Theory of Information Warfare: Preparing for 2020*. Maxwell: Air University, 1997.
Weber, N, A Belly, N Holzenberger, R Rudinger, and B V Durme. Human scheme curation via casual association rule mining , 2021.
Zaighum, Z, and F Rasool. Mapping Fault lines in the context of Hybrid Warfare: A Case Study of Pakistan. International Review of Social Sciences, 2021.