BIPSS Commentary
www.bipss.org.bd May-2024
BIPSS Towards a Secure World

Influence Operations: New Frontier in Warfare

Fahad-Al-Salam[1]

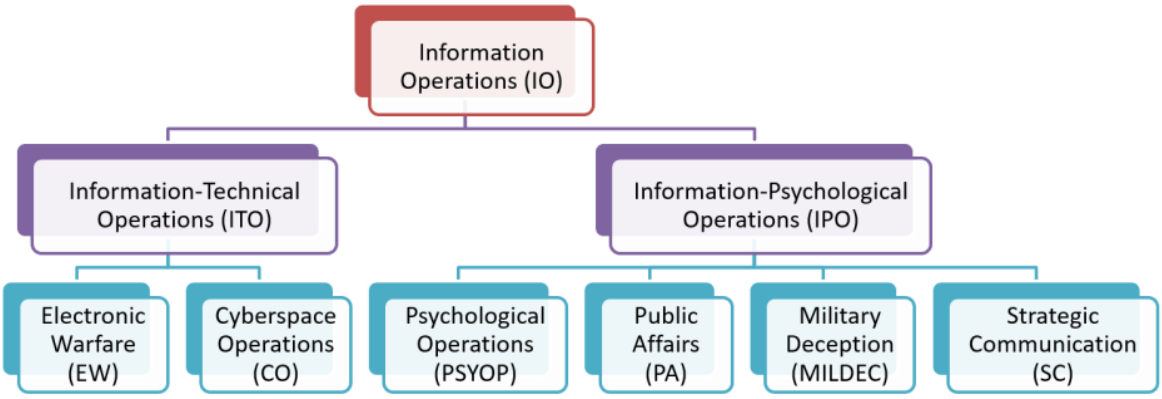
(Source: Air power Asia)

Introduction

From the traditional mode of warfare, the shift towards a more unconventional form of warfare has added a new dimension where the issue of proximity has become less relevant. Conflicts can now be waged across borders and within the digital realm, blurring the lines between war and peace, and challenging traditional notions of sovereignty and territoriality. The networks created around the world have made people's lives easy on one hand; but on the other hand, it has increased the vulnerability of anything that is connected to a network. As Rod Beckstrom, former director of the United States Cyber Security Centre said, "Everything attached to a network can be hacked; everything is being attached to networks, therefore everything is vulnerable".[2] The

[1] Fahad-Al-Salam is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). He completed his BSS (honors) and MSS from the Department of International Relations, BUP.
[2] Goldstone, Charlotte. "The 'Double-edged Sword' That Makes Shipping an 'easy Target' for Cyber Crime - the Loadstar." The Loadstar, October 17, 2023. https://theloadstar.com/the-double-edged-sword-that-makes-shipping-an-easy-target-for-cyber-

conventional tactics are still important, but influence operations, psychological warfare, and information operations- whatever someone calls it- is a crucial instrument for influencing geopolitical results without resorting to the use of physical force. There are many forms of influence operations. It can range from direct cyber-attacks to indirect operations like spreading disinformation and propaganda, social media manipulation, and information warfare. The following figure provides a glimpse of how these operations run.



(Source: Future Wars)

In this commentary, the transition of the modes of warfare will be discussed first. Secondly, how different platforms such as traditional media, social media, and cyber operations spread are used to conduct these operations and their effectiveness will be discussed. Lastly, how the state and non-state actors conduct these operations will be discussed.

The Shift in Warfare

With the advent of cyberspace, there is a clear shift in modern warfare. The issue of "dual use" is quite significant in case of technology. When a country buys a fighter aircraft, there is always an opportunity that it will be used for military purposes. It is the same in the case of information technology systems. Just like the invention of dynamite by Alfred Nobel, when information technology is developed, there is always a possibility that it will be used by the wrong people for

crime/#:~:text=%E2%80%9CEverything%20attached%20to%20a%20network,United%20States%20Cyber%20Security%20Centre.

wrong intentions.[3] At the same time, these networks can be hacked. As a result, the issue of vulnerability discussed by Rod Beckstrom can prove to be very dangerous not only for a country's military base but also for any type of infrastructure of the country.

Next, the number of adversaries in this digital age is unknown. Previously, the kings or leaders could measure the number of their enemies. But in this cyberspace, anyone can be an enemy and there is no fixed number for that. As proximity has become irrelevant, the attacks can come from anywhere, they can come from terrorist organizations, criminal groups, businesses no one knows about, or anonymous accounts. There is no such thing as a warning. In the early days, the leaders used to get warnings from their informers before an attack was incoming. But in cyberspace, whenever someone or something is being attacked, the earliest one can realize is at the time when the attack is happening.

The perpetrators can even use proxies to accomplish their tasks. As a result, no one can find the actual source from where the attack has been conducted. As a result, even after an attack, a state or a person, or an organization does not have a clue where the attack has come from. They just assume it and as a result, sometimes the actual perpetrator gets away.[4]

One thing is certain, that in cyberspace, offence is far easier than defense. Unlike the traditional warfare, defending an attack is very difficult compared to conducting an attack and that is because, the source of an attack and the number of attackers are unknown and the use of proxies can easily create doubts about who is the actual attacker. That is how cyberspace has given rise to a more complex warfare.

Different Platforms of Influence Operations

Traditional Media: Traditional media has long been functioning as a platform for influence operations. Television, radio, news channels, posters, magazines, books have been playing a key role in these operations. It has both short-term and long-term effects. Traditional media has the

[3] "Dynamite and the Ethics of Its Many Uses - American Chemical Society," American Chemical Society, n.d., https://www.acs.org/education/outreach/celebrating-chemistry-editions/2021-ncw/dynamite-ethics.html#:~:text=Nobel%20created%20dynamite%20to%20help,and%20damaging%20buildings%20during%20war.

[4] "Cyberspace: The New Frontier in Warfare," World Economic Forum, February 4, 2020, https://www.weforum.org/agenda/2015/09/cyberspace-the-new-frontier-in-warfare/.

capability to set an agenda.[5] The beneficiaries of these influence operations try to set the agenda according to their advantageous position. At the same time, setting propaganda through the traditional media is quite easy and people tend to believe these sources more. From elections and wars to personal benefits, these sources can play a huge role in influence operations. The role of traditional media was immense in stopping the Vietnam War. The Gulf War exemplifies how traditional media can be effectively employed to influence operations during warfare. By controlling the narrative through television, print, and radio, both the coalition and Iraqi forces aimed to shape perceptions, boost morale and achieve strategic objectives.[6] The extensive use of media during this conflict set a precedent for how influence operations are conducted in modern warfare.

Social Media: Social media has now been one of the key sources of influence operations as it is cheaper and easier to access. Social media provides a free platform for people to express their views and opinions. The "social media soldiers" use this opportunity and many of them conduct "citizen journalism".[7] Manipulation has become very easy through this as they carry almost the same weight as the mainstream media. Although there are a lot of fact-checking platforms, in the flood of disinformation and misinformation, it is not possible to keep pace with those. The ongoing Russia-Ukraine war is a huge factory of influence operations where both of the parties are using mainstream social media platforms to shape public opinion and international perception. A cyber war is going on between these two warring parties and social media is playing an influential role in that.

[5] Jon Bateman et al., "Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research," Carnegie Endowment for International Peace, June 28, 2021, accessed May 26, 2024, https://carnegieendowment.org/research/2021/06/measuring-the-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research?lang=en.
[6] Barbara Allen et al., "The Media and the Gulf War: Framing, Priming, and the Spiral of Silence," *Polity* 27, no. 2 (December 1, 1994): 255–84, https://doi.org/10.2307/3235175.
[7] Kathryn Ames, "'Citizen journalism', the military and the media," *Australian Defence Force Journal*, no. 193 (January 1, 2014): 20, https://search.informit.com.au/documentSummary;dn=450126503290203;res=IELAPA.

(Source: Center for Land Warfare Studies)

Cyber Operations: Cyber operations during warfare have become an integral part of modern conflict, often used to complement traditional military strategies. These operations can include cyberattacks on infrastructure, espionage, information warfare, and disruption of communication systems. Stuxnet, a highly advanced computer worm which is regarded as the world's first cyber weapon, gained widespread attention in 2010. Primarily, Stuxnet aimed to disrupt the centrifuges in Iran's uranium enrichment facilities, intending to covertly hinder Iran's developing nuclear program. Over time, the worm was adapted to also target other critical infrastructure, including gas pipelines, power plants, and water treatment facilities. Stuxnet destroyed nearly one-fifth of Iran's nuclear centrifuges, infected over 200,000 computers, and caused physical damage to about 1,000 machines.[8]

These are the top three platforms of influence operations. Besides these, there are other platforms like bots and troll farms which have become very influential nowadays which have their unique capabilities.

Actors of Influence Operations

State Actors: Influence operations in warfare by state actors are complex and multifaceted, blending traditional propaganda with modern cyber tactics to achieve strategic goals. In any war, a state wants to defeat its adversary by any means. In the present context, influence operations are quite influential and an easy option for states. Although it is not new. Even in the two world

[8] "Stuxnet Explained: What It Is, Who Created It and How It Works," www.kaspersky.com, April 19, 2023, https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet.

wars that the world has undergone, these operations were present; the only difference now is the advancement of modern technology has made it even more sophisticated and easier to disseminate. These operations are designed to shape the information environment, manipulate perceptions, and exert control over both domestic and international audiences. It is not something new that states have conducted influence operations to promote their values and ideals.

During the Cold War era, the United States of America used various traditional media platforms to promote its ideals. The Voice of America (VOA), for example, used to broadcast content promoting American values in the name of countering the Soviet propaganda against the USA.[9] The impacts were huge in shaping the public perception of the war towards the USA.

China, through its media and diplomatic channels has constantly been promoting its claims over the South China Sea. China claims a large portion of the South China Sea, demarcated by the so-called "Nine-Dash Line," which covers most of the sea. This claim includes areas near the coastlines of other Southeast Asian countries, based on historical maps and records.[10] The South China Sea is a bone of contention between China and some other countries such as the Philippines, Vietnam, and Taiwan and the US is supporting them on their claims. China's claim of having control over the whole South China Sea is being propagated through state-sponsored media and other diplomatic channels. This is how China is strengthening its position in the South China Sea.

Nowadays with the widespread use of social media, promoting a state's value and its position has become easier.

Non-State Actors:

Non-state actors (NSAs), including terrorist groups, insurgents, private military companies (PMCs), and hacktivist groups, are increasingly influential in modern warfare. These actors often employ influence operations to achieve strategic goals, shape public perception, and undermine their adversaries. Terrorist organizations, insurgent groups, Private Military Companies, transnational criminal organizations, cyber activist groups, and perpetrators of ideological

[9] John B. Whitton, "Cold War Propaganda," *American Journal of International Law* 45, no. 1 (January 1, 1951): 151–53, https://doi.org/10.2307/2194791.
[10] "Territorial Disputes in the South China Sea | Global Conflict Tracker," Global Conflict Tracker, n.d., https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea.

movements are all part of NSAs. In many cases, these groups are more active in conducting influence operations than the states. As in most cases, these organizations fight against a bigger entity, they need the support of the masses to ensure that they conduct these operations very actively. From recruiting people to their organizations to gain global sympathy and support for their cause, these organizations use social media and traditional media to show their perception of the world and try to prove the legitimacy of that.

The Islamic State of Iraq and Syria (ISIS) was very efficient in conducting these operations. As former US President Barack Obama said about ISIS that they are "very savvy when it comes to social media, and able to infiltrate the minds of... disaffected individuals around the world".[11] Even after killing thousands of people which had also gone viral on social media, lots of people were still joining the group, even after knowing very little about Islam. This is the capability of influence operations; if someone knows how to maneuver it well, gaining support becomes very easy through spreading propaganda.

In the case of Russia's paramilitary Wagner group, influence operations were conducted through social media like Twitter and Facebook. To gain support and as a recruitment strategy, they provided job ads on these two platforms and the views went up to more than 120,000 on these platforms, according to a U.K. disinformation-focused research group. [12] They were very active on social media and used to post in dozens of languages where they even mentioned the salary along with other health benefits.

Nowadays, almost every NSAs use the social media platforms to conduct influence operations. On the one hand, it is easier and cheaper and on the other hand, it is very effective. That is why, they stay very active on these platforms.

[11] Gerstel, Dylan. "ISIS and Innovative Propaganda: Confronting Extremism in the Digital Age." *Swarthmore International Relations Journal*, no. 1 (January 1, 2016): 1–9. https://doi.org/10.24968/2574-0113.1.5.
[12] Clothilde Goujard, "Russia's Wagner Group Uses Twitter and Facebook to Hunt New Recruits," *POLITICO*, May 31, 2023, https://www.politico.eu/article/russia-ukraine-war-mercenaries-wagner-group-recruit-twitter-facebook-yevgeny-prigozhin/.

Conclusion

The shift in warfare because of technology was certain and influence operations are one of the significant results of that as well as a new means of modern warfare. These operations leverage various platforms to shape perceptions, spread disinformation, and manipulate public opinion. The digital age has introduced new vulnerabilities without direct military confrontation. Their ability to impact geopolitical outcomes without physical force underscores the need for robust countermeasures and a comprehensive understanding of this unconventional threat. As technology advances, the importance of safeguarding information environments and maintaining resilience against such operations becomes ever more critical.