Published on *USC Center on Public Diplomacy* (https://uscpublicdiplomacy.org)

Thumbnail Image:

Mar 04, 2023 by Jorge Marinho

Influence Operations, Ontological Security and (Counter)Intelligence [1]

Note from the CPD Blog Manager: *An earlier version of this piece was published on Feb 14, 2023, in Marinho Media Analysis here.*

Introduction

This article is based on bibliographic research and, chiefly, exclusive interviews with the following experts: Christopher Paul, Jahara Matisek, James Farwell, Jennifer Counter and Petros Petrikkos.

As part of this piece, it is vital to take into account the concept of influence operations. In general, every activity conducted by states or by any other groups, in both times of peace and wartime , including the grey-zone context, with the aim of influencing a target audience. Specifically, this article is centered on the influence exerted on certain audiences, depending

on the messages/narratives conveyed through various channels, such as traditional and social media.

Influence operations can encompass information operations. According to several authors, oftentimes the terms information operation and information warfare are used indiscriminately, that is, as synonyms. There is a variety of terms that can generate confusion: psychological operations, influence operations and information warfare . In all of this, there is a common goal that this article focuses on: influencing.

How, and to what extent, can influence warfare, chiefly in the medium to long term, jeopardize a country's ontological security?

Target(s)

Among various aspects, intelligence services can provide details regarding targets of information operations. In the words of Jahara Matisek, the Information Operations Division at U.S. Northern Command (USNORTHCOM) (J39) seeks to cooperate with the intelligence community, when it comes to defending the American homeland against opponents' campaigns and promoting American values in the Western Hemisphere.

The targets of influence operations could include large swaths of the population of one or several countries, groups of people or an individual. From Matisek's standpoint, this latter case could end up being part of the next major conflict, given that, in reality, few Western citizens are ready to face well-structured adversarial operations that could go by way of direct messages (DMs) of various social media.

According to Jennifer Counter, if an influence operation comprises a narrow goal, the target can be a small group or a single person. Counter considers that, in this age of social media and microtargeting, it is easier than ever to address key messages to a target audience comprising a small number of people.

Selecting foreign individual targets and channels precisely for sending them the messages constitutes relevant aspects of influence warfare. Matisek stresses that artificial intelligence enables gathering data found in the public sphere on an individual and, based on this, sending him/her messages that have been created specifically for him/her.

Ontological Security

How, and to what extent, can influence warfare, chiefly in the medium to long term, jeopardize a country's ontological security? In this regard, Paul is not unaware that, on the one hand, there are those who do not assign a great deal of importance to foreign malign influence and, on the other hand, there are also those who, in said influence, see a potential existential threat.

Petros Petrikkos states that, in the case of a conflict between nations, information/influence warfare can be used by one of the parties to disrupt the regular functioning of the other State

and of society in general, thereby calling ontological security into question.

Counter points out that influence operations can be very dangerous when they seek to gradually weaken aspects that serve as the basis of society, such as shared histories, values and norms. From an offensive standpoint, Counter believes that casting doubt on foundational ideas can somehow serve to create divisions between citizens and their State, between people of different groups in society (in religious and ethnic terms, for instance) and among family members or a circle of friends.

Both James Farwell and Counter agree that, in reality, the existence of barriers to freedom of expression, information and the free entry of messages from foreign countries hinders influence operations geared to a given country via the media. From Petrikkos' viewpoint, when the State imposes limits to information, it could potentially cause a negative effect on its citizens, for example, by causing reduced trust in Government.

Resilience

From Matisek's perspective, a certain country's social resilience constitutes a hindrance in relation to threats of psychological warfare. He feels that, currently, any society should invest in digital literacy, critical thinking and civic education. Matisek advocates that every citizen's involvement in national defense allows for both individual and collective strengthening that will serve to withstand adversarial influence activities, among other aspects.

In order to deal with situations such as psychological warfare, propaganda or disinformation, Christopher Paul also maintains that fostering individual and collective resilience is important. From the viewpoint of this RAND Corporation expert, one of the factors that can somehow contribute toward said resilience is media literacy, even though, relative to its efficacy, contradictory research outcomes may emerge. According to Paul, another measure against said situations could include inoculation or pre-bunking, where potential targets are pre-seeded with lighter propaganda arguments and counterarguments.

Counterintelligence

In relation to the activities conducted by counterintelligence services to prevent influence/psychological operations in their countries, Counter maintains that, first, we need to understand that influence operations and campaigns comprise an end goal. According to Counter, an overview may be lacking, when too much attention is often paid to certain specific contents, such as a tweet or a given account on social media. She states that rarely are content batches compiled in order to grasp the message and be aware of the targeted key public, subsequently reversing the process so as to understand the actor and his/her goal.

According to Matisek, even though few governments and military organizations publicly disclose offensive or defensive operations, in the sphere of influence/psychological warfare, states generally apply some resources in identifying potential adversarial influence attacks. This type of counterintelligence activities, according to Matisek, goes by way of analyzing trends, attempts to put an end to inflammatory information and collecting foreign IP addresses, for instance. Surely, when fighting influence/information operations, the state's role is relevant, mainly with regard to its counterintelligence agencies.