INFORMATION WARFARE

Jorge Marinho *addresses various aspects related to influence operations, such as targets, social and individual resilience, ontological security and (counter)intelligence*

This article addresses various aspects related to influence operations, such as targets, social and individual resilience, ontological security and (counter) intelligence. The internet and Artificial Intelligence, as well as a few aspects with regard to training future information/psychological warfare professionals are also highlighted. This work results from the bibliographic research and exclusive interviews with a variety of experts. 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 gray-zone context, with the aim of influencing a target audience. Specifically, this article is centred on the influence exerted on certain audiences, depending on the messages/narratives conveyed through various channels, such as traditional and social media. According to several authors, often 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 this, there is a common goal that this article focuses on: influencing (Information Operations/ Psychological Warfare).

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

For US military operations, intelligence and information operations are crucial components, with information comprising the essence of both communities. There has to be a high degree of coordination between those backing intelligence support and whoever plans and executes operations in the information environment. Among various aspects, intelligence services can provide details regarding targets of information operations.

In the words of Jahara Matisek, the Information Operations Division at US NORTHCOM 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. This National Security Affairs department professor at the US Naval War College adds that, in relation to US intelligence agencies and military units involved in information/psychological warfare, there could be some sharing of the best practices and ways of identifying adversarial actions.

The targets of influence operations could include large swathes of the population of one or several countries, groups of people or an individual. From Jahara 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. James Farwell states that, currently, within the sphere of influence operations, individual targets are important.

According to Jennifer Counter, if an influence operation comprises a narrow goal, the target can be a small group or a single person. This expert points out that, for the sake of efficacy and efficiency, it is vital to have a good understanding of the key public. 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 for precisely 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 them. This way, according to Matisek, as part of psychological warfare, a different reality can be socially and digitally constructed, in the infosphere of the individual target with which he/she coexists.

James Farwell, Jahara Matisek and Christopher Paul all point out that there is increased intensity and breadth of information/psychological operations, when these are automated, namely with the use of socialbots. This, according to Matisek, can be dangerous, when looked at as entailing a relatively low cost and with hardly any risks, given that there are no precedents for this type of actions on the international system, as to drawing red lines; thus, the likelihood of a conventional military response is low, at least up to the present moment.

Also in the sphere of the internet, Farwell believes that, without generalising, troll farms/factories can be effective, when strongly affecting certain sites and through clever social media. In the opinion of Christopher Paul, troll farms play a relevant role, as part of foreign malign influence, thus allowing a government or group to take advantage of individuals' power to manage the contents of a much larger number of people and accounts that are fake.

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. For this to happen, when dealing with a systematic process, Petrikkos feels that information resources and time are needed. They explain that, first off, information is gathered on the target country, to identify and subsequently exploit its vulnerabilities. According to Petrikkos, a target, with its functioning disrupted and with no resilience, becomes insecure and more permeable to influences, with regard to its identity.

IN THIS AGE OF SOCIAL MEDIA IT IS EASY TO ADDRESS KEY MESSAGES TO A TARGET AUDIENCE

Jennifer Counter feels that the narratives that guide who we are and the position we take up within a group are very powerful, to the extent that identity is an essential part of the individuals and the society we live in. This is why, she 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. According to Counter, part of warfare includes determining target audiences and the messages that gradually destroy societal narratives, thus contributing to, for example, undermining an adversarial government's credibility.

Various experts, including Christopher Paul, Jahara Matisek, James Farwell and Jennifer Counter, acknowledge that, on the international stage, influence operations geared to certain countries already dealing with some social, political and economic problems, possibly combined with involvement from certain local leaders, can contribute toward triggering or heightening uprisings.

From Jahara Matisek's perspective, a specific country's social resilience constitutes a hindrance in relation to threats of psychological warfare. This officer feels that, currently, any society should invest in digital literacy, critical thinking and civic education. With regard to this, Matisek points to Sweden and Finland as two countries that are exemplary in addressing psychological warfare, strengthening their societies, in order to triumph over malign actors seeking to cause divisions through disinformation and misinformation. He explains that, with similarities, the models of the two countries mentioned, respectively Total Defence and Comprehensive Security, present an overview regarding security and national defence, to the extent the elements of the public and private sectors are aware

of the role they need to play in a crisis situation. This professor advocates that every citizen's involvement in national defence allows for both individual and collective strengthening that will serve to withstand adversarial influence activities, among other aspects.

Christopher Paul underlines that more effective counterpropaganda strategies should consider every stage of propaganda. Several researchers conclude that, in order for malign or subversive information to be effective, it must successfully go by way of the stages of production, distribution/redistribution and consumption. This is why, with a far-reaching perspective, the fight against said types of information shall concern every stage, not just in consumption, as is the case with fostering resilience, even if such is somehow positive .

TARGETS OF INFLUENCE OPERATIONS CAN INCLUDE ONE OR SEVERAL COUNTRIES

In relation to the activities conducted by counterintelligence services to prevent influence/psychological operations in their countries, Jennifer Counter maintains that, first of all, 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 a social media. This expert 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 Jahara Matisek, even though few governments and military organisations 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 analysing trends, attempts to put an end to inflammatory information and collecting foreign IP addresses, for instance.

Jennifer Counter maintains that influence operations are more art than science. Among the multiple subjects that comprise training a future information/psychological warfare professional, she stresses political science, behavioural science, psychology, history, geography, anthropology, languages, social movements and measurement approaches (pooling, surveys and focus groups). James Farwell considers that a future information/psychological warfare professional should have talent and study hard, most notably cyber operations. As part of this, Jahara Matisek feels that a cyber professional, within the context of sociopolitical-information warfare, should be dynamic enough to understand a diversity of cultural, social, political and historical trends. Matisek adds that, from his standpoint, said professional should have characteristics that include a free spirit and an ability to come up with out-of-the-box solutions ●

Jorge Marinho has a PhD in Communication Sciences and BA in International Journalism. His main fields of expertise include: influence/information, psychological warfare; international communication, international relations and strategic communication.

Information is gathered on a target country to identify and subsequently exploit its vulnerabilities