SOCIAL ENGINEERING – MAJOR COMPONENT OF COGNITIVE WARFARE –

Colonel Claudiu Marius IONESCU

Major General (r.) Florian RĂPAN, PhD

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2022.3.03

Industrial revolutions have generated major changes in the economy, politics and military affairs throughout human history and have led to innovation in all social fields, resulting in new approaches to military affairs. Companies are transforming and preparing their transition from an environment based on technological tools (physical) to one based on social mass engineering (mainly in the virtual environment), extremely refined, which subtly combines manipulation with addiction.

The industrial society, as we have known it for more than a century, has become an information society and produces major changes in society and, implicitly, in the thinking of military strategies. In this context, due to the unprecedented development of information technology, the military confrontations of the future will change their main feature, namely violence, a component that will be increasingly mitigated and replaced, gradually, with non-kinetic means: political, economic, media, psychological and informational situations.

There are, today, new military doctrines and strategies, characterised by the lack of classical rules for waging a war, through the ambiguity of the enemy or through the lack of dichotomy between war and peace, which have as characteristic another way of organising and conducting the fight.

The present article focuses on aspects related to non-kinetic and cognitive combat means. We consider that the research is of interest because the implications of these means on the way of waging the war and their long-term effects that have not yet been fully known. In this context, we approach the field of social engineering, starting from the first references to this concept up to the present day, emphasising its applicability in social and political sciences as well as in psychology and cyber security.

Keywords: social engineering; cognitive warfare; strategic warning; cyber-influence; strategic manipulation;

ROMANIAN
MILITARY
THINKING

INTRODUCTION

In the current conflict, with increasingly asymmetrical tendencies, the development of neuroscientific techniques and means as neuroweapons increases the possibility of manipulating the human mind, this being the next battlefield of the 21st century (Du Cluzel, 2020, p. 12).

The human being is naturally attentive and oriented towards the danger of external threats, physically felt (physical attacks, chemical pollutants, radiation, biological agents), which people can consciously control, through prevention. Human beings have not yet reached a level of instinct development that allows them to be automatically aware of the subtle danger of psychological contamination (David, 2017, p. 2). Thus, one of the major mistakes we make, as a species, is not to be aware of the danger of psychological aggression. We generally believe that exposure to false or misleading information is not a danger, as we can distinguish between true, false or misleading information and that, thus, we can control the mental manipulation and the effects of this exposure. Neuroscience specialists contradict us: once exposed to false information, people can be influenced in their opinions. And this is because we have the illusion that we can control that information, which we have assimilated as true, and we do not make the effort to verify it. This mechanism is the basis of social engineering, successfully used in economic, political marketing, as well as in non-kinetic aggression of cognitive type.

We generally believe that exposure to false or misleading information is not a danger, as we can distinguish between true, false or misleading information and that, thus, we can control the mental manipulation and the effects of this exposure. Neuroscience specialists contradict us: once exposed to false information, people can be influenced in their opinions.

This paper shows the importance of studying social engineering used in cognitive warfare, as well as the possibilities for such aggressions to be mitigated by strategic decisions.

THE UNSEEN WAR

Current digital technologies globally create the possibility for a democratic state, with strong armed forces, to easily become the target of a terrible war, even if it were an apparent state of peace. The targeted state may not anticipate the extent of the attacks

and can be overwhelmed before it realises that it is in a war (Sherr, 2015). All this can be done today without the use of kinetic force, but only through tools of social engineering and with the help of information technology, as follows: through strategic manipulation, by influencing the population and leaders and by cyber-influence actions. The author of these types of operations can be a state or non-state entity, which has the advantage of expressing itself under anonymity, mainly in the virtual space, an environment in which it is difficult to identify the source of aggression. These actions are therefore below the perception threshold of the assaulted state and of some intentional political and military organisations of which it is a part.

The high communication speed, the low cost of social engineering actions (disinformation, influence, strategic manipulation, cyber) and the efficiency demonstrated in recent conflicts generate a growing trend of "cyber-cognitive" attack methods. In these types of conflicts, "social media" and "Big Data" platforms play a crucial role, being an important source of information.

Analysing, in general, the purposes of a war – namely its financial, economic, political, ethnic, or geostrategic interests – we can say that, to have access to a state's resources or to transform it into a commercial area for own products, to impose own political interest on it, there is currently a series of subtle possibilities entailing cognitive actions on a population of interest. They are much more effective in terms of persistence of effects and less expensive than conquering its territory using the armed forces. They are mainly moved into the virtual environment, which allows them to circumvent physical boundaries and facilitate the access of an aggressor entity, whether state or non-state, to the target population as well as to its institutions and services. Today's digitalised society is expanding and improving the possibility of data acquisition, providing the opportunity to either defend own data or disrupt those of the enemies.

Also, the high communication speed, the low cost of social engineering actions (disinformation, influence, strategic manipulation, cyber) and the efficiency demonstrated in recent conflicts generate a growing trend of cyber-cognitive attack methods. In these types of conflicts, social media and Big Data platforms play a crucial role, being an important source of information.

SOCIAL ENGINEERING IN THE DIGITAL AGE

The emergence of social engineering has been closely linked to the evolution of social sciences. The first references to the concept of social engineering, published about 150 years ago, are attributed to Charles Fourier, a French sociologist and economist, and to the French engineer Émile Cheysson. They considered social engineering as a branch of applied sociology and proposed it as a tool for creating

an ideal society that would prevent and resolve social conflicts. Over time, social engineering has evolved a lot, haing a wide range of applications within social sciences, political science, in the framework of cyber security, as well as in psychology.

In France, social engineering is considered a beneficial tool for society. Institutions such as the University of Toulouse, the Regional Institute of Social Engineering (*Institut regional d'ingénierie sociale* – IRIS) and the Regional Institute for Social Assistance (*Institut régional du travail social*) offers state diplomas in social engineering, graduates becoming specialists in modelling the social environment.

Some applications of social engineering are mainly directed against people and not in support of them, the new tendency being to militarise this social instrument, namely to adapt it for military purposes. Social engineering is also assimilated into *"social influence"* and oriented towards changing social options and manifestations, without constraints, in the form of persuasion, manipulation or indoctrination, to obtain political, economic or/and military advantages.

In fact, at this stage of civilisation, all areas of social life are influenced by social engineers. It involves the application of diversified *"policies"* (social or scientific), in the economic, demographic, educational and cultural fields, to manipulate public opinion. Currently, social engineering is carried out through modern methods employing *brain piracy* (or *neuro-piracy*), passing through epigenetic programming as well as through semantic and socio-cultural environment (Cerise, 2018). By the *"militarisation of brain sciences"* a new type of conflict was developed, called cognitive warfare (Du Cluzel, p. 25). It is carried out by exploiting the vulnerabilities of the human brain and by sophisticated social engineering, so that at least part of the targeted society behaves according to one of the opponents' plans.

Some applications of social engineering are mainly directed against people and not in support of them, the new tendency being to militarise this social instrument, namely to adapt it for military purposes. Social engineering is also assimilated into "social influence" and oriented towards changing social options and manifestations, without constraints, in the form of persuasion, manipulation or indoctrination, to obtain political, economic or/and military advantages.

PSYCHOLOGICAL MANIPULATION

As stated above, the human being has not yet reached the level of development allowing them to be aware of the hidden danger of psychological contamination. That is why rational thinking does not come naturally, but requires effort and involvement (David, ib.).

The processing and classification of information in the human brain begins with the upload of information on the biological hard drive, namely our mind. Naturally, at this stage, any information

is considered by the brain to be true if we do not intervene by analysing and classifying the information as true or false (ib.).

In general, psychological manipulation is based on blocking exposed people from analysing the veracity of the information to which they are exposed. This type of manipulation can be performed as follows:

- by subliminal transmission of information (below the sensory threshold);
- by *"bombarding"* with a large amount of information that cannot be critically analysed because of limited memory resources;
- in periods of advanced brain fatigue, when the brain is distracted, involved in other tasks, so that memory and attention resources are focused in another direction;
- when the information comes from a source that we consider credible, and we decide to suspend the analysis.

According to specialists, cognitive warfare means the use of knowledge and information processing capabilities for conflicting purposes. The influence of human knowledge requires a large amount of detailed personal information to identify influential individuals or to perform influence operations, depending on the characteristics of subgroups of people.

We are usually not aware that, when information is false or misleading, it can contaminate us mentally, unconsciously influencing our decisions. Thus, neuroscience specialists have concluded that, once exposed to such information, we are already influenced, even if we are aware of its quality and believe that we have blocked it, and consequently, its effects on our emotions, cognition and behaviour. Their recommendation not to be manipulated is to consciously and permanently check and control if the decisions made belong to us.

THE WAR FOR OUR MIND

Today, after almost three decades of conflicts in the information age, discussions about cognitive warfare still seem an unrealistic paradigm of thinking about the security of a state. Is it possible, however, that the height of information technology means that future wars will take place mainly in the cognitive field?

According to specialists, cognitive warfare means the use of knowledge and information processing capabilities for conflicting purposes. The influence of human knowledge requires a large amount of detailed personal information to identify influential individuals or to perform influence operations, depending on the characteristics of subgroups of people.

Cognitive warfare mobilises a wide range of strategies, tools, and techniques to gain control in environments of interest. It aims to influence the brains of members of the target population (civilians

or military), the victory being given by the ability to impose the desired behaviour on the interest group. The long-term effects of this type of warfare are, in most cases, unknown. However, it generates major advantages by using sciences such as nanotechnology, biotechnology, information technology, cognitive sciences, as well as neuroscience, by adapting them to the purposes of war, by *militarising* them.

Hyper-connectivity has, in this type of conflict, the major role of a Trojan horse. With it begins the cognitive warfare, because, at present, almost everyone has a mobile phone connected to the internet. In the same context, *information* is the fuel of this type of war. Cognitive warfare is therefore the science of using technologies to transform the human targets knowledge (Du Cluzel, ib.). These technologies incorporating the NBIC fields (nanotechnology, biotechnology, information technology and cognitive sciences) (Roco, Bainbridge, 2002, p. 2) far exceed through complexity the information warfare or psychological operations, because they do not generate a struggle for information, but a struggle to take control of the brains of individuals who are part of the target group.

Cognitive warfare is therefore the science of using technologies to transform the human targets knowledge. These technologies incorporating the NBIC fields far exceed through complexity the information warfare or psychological operations, because they do not generate a struggle for information, but a struggle to take control of the brains of individuals who are part of the target group.

We can no longer discuss cognitive warfare today without considering *social media*, heavily supported by the technologies and resources of Big Data corporations as well as by Artificial Intelligence. Big Data resources are needed to gain access to data on individuals, groups, or companies of interest, for better knowledge, to change the way of thinking within the target group.

An example may be China, which has assimilated over the years a massive amount of personal information about US government officials, but also about ordinary citizens. Thus, it is currently expected that Chinese IT giants have a sufficiently large database to influence people's knowledge (Dorfman, 2020) and generate in areas of interest, especially in Taiwan and Hong Kong, aggressive and coercive actions to influence the population (Insikt Group, 2020).

The first conflict in which the cognitive dimension of war is evident is the war in Ukraine. Although the conflict is seemingly kinetic, the actors involved try to shape the information environment and, implicitly, the opinions and behaviour around the world, through the widespread use of Big Data as well as social media.

Cognitive warfare through social engineering can create false alternative realities in democratic states, favoured by their freedoms (freedom of speech or free communication of ideas). Thus, reality

and truth can be perverted, using a mix between the specific elements of propaganda and a series of facts, sophistry, and untruths. This creates an alternative reality that can lead the targeted population to perceive a predefined model.

Cognitive warfare is a type of conflict generated by changes in the characteristics of war, the violent character being replaced by actions with low physical, non-kinetic, impact. Thus, the war has become predominantly informational, supported by an unprecedented development of information technology and social sciences.

There is also the concept of *"War 2.0."* (Afrem, 2019), a term related to the digital character of current military technology, as well as the theory that wars are no longer won only in trenches but also in front of the computer, through information technology and *"cognitive battle"* (of brains). It entails the use of social engineering actions, such as diversion, manipulation, misinformation, or the use of cognitive distortion (errors of logic), distortion of reality. In this way, everyday reality can be *"altered"* by changing people's opinions with the help of technology.

Today, cognitive warfare is one of the main aggressions of a state. It is a form of conflict specific to the 21st century, an effective deterrence tool at the strategic level, which can be used both globally and in zonal conflicts, in different areas of operations.

Today, cognitive warfare is one of the main aggressions of a state. It is a form of conflict specific to the 21st century, an effective deterrence tool at the strategic level, which can be used both globally and in zonal conflicts, in different areas of operations.

Although it seems to be a modern type of war, the issue of cognitive warfare is not new. The effects of weakening political power and institutions of force in a state have been known for thousands of years. It is totally different from the classical one, because most of it is mainly conducted through subversive actions, in order to weaken the power, by demoralising the population and the staff of the structures involved in national security, by destroying the population's trust in them, generating social polarisation. It synergistically encompasses social engineering and the power of digital technologies. Every war or conflict has perfected it, reaching that, in the last century, with the technological revolution in the field of communications, it became considered by military thinkers as a distinct type of war domain, as important as the other known ones (land, air, sea, space).

Cognitive warfare is not mainly based on military equipment, it requires fewer resources and, at the same time, may have greater remanence over time. It can guarantee success even for small states.

It can generate solutions to resolve conflicts with minimal losses and destruction by initiating military operations in which the targets can be: *undermining the beliefs of the opponent's leaders, encouraging, giving up, taking over, or destroying enemy command and control systems.* Also, in contrast to the undesirable effects of kinetic operations, which require deployments of forces and constitute a risk to one's own forces, these types of cognitive military operations can be safely conducted remotely, from own bases, for long periods of time and with minimal risks to own forces.

CONSEQUENT MEASURES

Mass social engineering used in a cognitive warfare is difficult to anticipate, locate or counteract. There is a need to reduce one's own vulnerabilities and dysfunctions so that the impact of these influencing actions can be minimal. There is also a need to develop functional strategic warning systems at all levels.

Mass social engineering used in a cognitive warfare is difficult to anticipate, locate or counteract. There is a need to reduce one's own vulnerabilities and dysfunctions so that the impact of these influencing actions can be minimal. There is also a need to develop functional strategic warning systems at all levels.

In general, in such a conflict, the measures that can be taken against social engineering are reduced, open societies having the most vulnerabilities. Therefore, first, it is necessary to identify internal dysfunctions and vulnerabilities which, exploited by the enemy, can generate major risks. To this end, a functioning strategic warning system must be developed by generating predictive and pre-emptive analysis capabilities, allowing the state to know hostile actions in advance and to minimise the effects. This type of analysis is also known as *"strategic intelligence"*[1]. It must focus on identifying the specific causes of risk situations, the elements that determine their evolution and the variants of manifestation, and must constitute the necessary foundation for the generation of measures against information aggressions.

Strategic warning is a safe measure to reduce or stop the effects of operations in the range of mass social engineering when aiming at the severe destabilisation of a state.

Another important measure is the protection of one's own information. In this case, it is appropriate for the human resource to be competent and integrated. Careful verification of own staff is therefore needed to access classified information, as well as to create mechanisms to identify personal and professional vulnerabilities.

[1] The term *strategic intelligence* was launched by Sherman Kent in the work *Strategic Intelligence for American Policy – 1949*, being defined as *"the knowledge that political and military decision-makers must possess in order to ensure the national welfare"*.

One of the vulnerabilities may be the lack of security culture. In this context, the most effective defence against social engineering developed in an information warfare is AWARENESS. Every citizen (military or civilian) must be aware of the risks to him/her and the society to which he/she belongs. For this awareness to be effective, it is necessary to develop, from the central level, sets of rules and values (popularised among citizens) that will need to be protected and respected. There is also a need for the population to be trained regarding *the media*, to counter social engineering actions, such as propaganda and misinformation.

CONCLUSIONS

The future would increasingly be subject to social engineering, a capable and easy tool for achieving proposed goals, through manipulation, propaganda, and influence. To protect citizens (civilians and military) against psychological aggression, to create a high societal resilience, we must intervene with well-thought-out educational and psychological elements.

The human brain is constantly running a complex system, which operates, more often than not, autonomously, according to ancient rules. This system is extremely useful for those who know its subtle mechanisms and want to influence groups of people.

Attempts to influence some to others have always been a tendency of people in both civilian and military worlds. Politicians, traders, the military, managers, and other social categories involved in mass influence are looking for methods and solutions that are as effective and efficient as possible to solve their problems better, faster and at the lowest possible cost. These attempts will continue in the immediate future and will have an upward trend.

We can therefore expect that the future would increasingly be subject to social engineering, a capable and easy tool for achieving proposed goals, through manipulation, propaganda, and influence.

To protect citizens (civilians and military) against psychological aggression, to create a high societal resilience, we must intervene with well-thought-out educational and psychological elements. Also, a determined attitude in the fields of expertise of each person and the cultivation of basic social values decrease the possibility of being *"psychologically polluted"*.

World states will continue to strengthen their military supremacy with the help of kinetic capabilities but at the same time will be vulnerable to non-kinetic (cognitive) threats and mass social engineering respectively, which can turn these countries' population into a weapon at the fingertips of the enemy. In this context, we consider it appropriate for military decision-makers to focus on developing strategies to counteract the non-kinetic effects of the range of cognitive warfare against their own population (civilian or military).

BIBLIOGRAPHY:

1. Afrem, A.V. (2019). *War 2.0.* In *Intelligence Magazine*, https://intelligence.sri.ro/razboiul-2-0/, retrieved on 12 June 2022.
2. Cole, A., Le Guyader, H. (2021). *NATO's Sixth Domain of Operations*. Innovation HUB and Allied Command Transformation, https://www.innovationhub-act.org/sites/default/files/2021-01/NATO%27s%206th%20domain%20of%20operations%20%282%29.pdf, retrieved on 23 March 2022.
3. Cerise, L. (2018). *Neuro-pirații. Reflecții despre ingineria socială*. București: Editura Mica Valahie.
4. David, D. (2017). *Contaminarea psihologică – Manipularea* și *contaminarea mentală*. In *Sinteza*, https://www.revistasinteza.ro/contaminarea-psihologica-manipulare-si-contaminare-mentala, retrieved on 24 August 2021.
5. Du Cluzel, F. (2020). *Cognitive Warfare.* June-November 2020, https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf, retrieved on 23 March 2022.
6. Dorfman, Z. (2020). *Beijing ransacked data as U.S. sources went dark in China. As Xi consolidated power, U.S. officials struggled to read China's new ruler*. In *Foreign Policy,* 22 December 2020, https://foreignpolicy.com/2020/12/22/china-us-data-intelligence-cybersecurity-xi-jinping/, retrieved on 12 June 2022.
7. Eidelson, R. (2013). *Neuroscience, Special Forces and Yale.* 6 March 2013. CounterPunch.org, retrieved on 5 June 2022.
8. Gusterson, H. (2007). *The Militarization of Neuroscience.* In *Bulletin of Atomic Science*, 9 April 2007, https://thebulletin.org/2007/04/the-militarization-of-neuroscience/, retrieved on 5 June 2022.
9. Moreno, J. (2012). *Mind Wars. How the Military Want to Control Our Brains*, https://www.theguardian.com/books/2012/jun/01/mind-wars-jonathan-moreno-review, retrieved on 5 June 2022.
10. Roco, M.C., Bainbridge, W.S. (2002). *Converging technologies for improving human performance nanotechnology, biotechnology, information technology and cognitive science*. National Science Foundation. Arlington, Virginia, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/bioecon-%28%23%20023SUPP%29%20NSF-NBIC.pdf, retrieved on 4 June 2022.
11. Sherr, J. (2015). Clingendael Report. *The New East-West Discord. Russian Objectives, Western Interest*, The New East-West Discord-Clingendael Institute, https://www.clingendael.org, retrieved on 11 June 2022.
12. Insikt Group (2020). *Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests.* CYBER THREAT ANALYSIS 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0429.pdf, retrieved on 29 December 2021.
13. https://irtshdf.fr/irts/, retrieved on 12 July 2022.