# Information Strategies – Evolution and Influence to the Knowledge

Gordan Akrap and Đilda Pečarić

***Abstract***— What we investigate in this paper is a theoretical frame common to disciplines that research form of public knowledge, respectively common methodological approach to a series of activities that aim is not only to form public knowledge, but also have a the duty to provide information superiority. The proposed theoretical approach enables understanding and interpretation of the impact of modern information strategies (information and media operations (IO, MO)) on corpuses of public knowledge. IO and MO are focused on specific cognitive domains of target audience, and the effects of such formed information and communication systems have a direct effect on the organization of the targeted corpuses of (public) knowledge.

Low intensity conflicts (LIC) become the dominant form and way of dealing with international and local threats. The articulation of national information strategies should ensure political, economic, cultural and military domination of the actors on the global scene. National, as well as business, information doctrines and strategies define offensive and defensive methods and techniques of usage of information resources with aim to ensure information superiority. Superiority in weapons and lethal means is replaced by the superiority in the information and technical and technological development. Superiority in controlling and monitoring of the battlefield turned into a superiority and control of the media space. Battlefield is no longer dependent on space and time. Battlefields are media, and ICT space in which different IO/MO can last for 24 hours a day, 7 days a week, 12 months a year.

***Keywords***— Corpus of Public Knowledge, Information Strategies, Information-Communication Systems, Information Operations, Media Operations.

## I. Introduction

FROM the mid-20th century number of sciences and scientific disciplines that are involved in information and different types of knowledge are growing. J. Ziman [20] defined science itself as public knowledge. Information science is just one of the sciences engage in the organization and exchange of knowledge. Unfortunately the relationship between sciences that are engaged in information and knowledge are very loose, often are vague and theoretical concepts and methodological procedures are without cumulative effects. In other words, there is no recognizable mutual intellectual effort, direct theoretical relationship and methodological solutions between information science, librarianship and communication science with the disciplines that are involved in public relations (PR), media, journalism, knowledge management, information strategies, information operations, media operations, influence operations, etc.

Our starting thesis is that the subject of information science is necessary research of information strategies that shapes different corpuses of knowledge and therefore makes an influence of knowledge organisation and exchange of knowledge. This means that information science can and must deal with different corpuses of knowledge and influence of different information strategies to them. However, the assumption that knowledge is "dead", static corpus, stored in traditional libraries or modern repositories is incorrect. Corpuses of knowledge are living systems, "organisms" that move and change along with societies that create them under the influence of information attackers, use them, protect them, but they also discard knowledge very quickly, and especially information as obsolete.

In this paper, we tried to explore evolution of information strategies and their modus operandi through time, establish a links between several disciplines engaged in organization and exchange of knowledge. If information science aims to explore public knowledge (as defined by theorists of Information Sciences B. Težak [13, 14, 15], R. Capurro [7], T. Saračević [12], M. Tuđman [16]) then it would be logical to find a common methodological starting points with all disciplines and activities, that nowadays, have as primary task to influence and form public knowledge.

Therefore, in this paper we tried to offer also a theoretical framework that establishes relations between cognitive hierarchy of knowledge and different corpuses of knowledge: corpus of open knowledge and corpus of protected knowledge. Such a theoretical approach enables understanding and interpretation of the impact of modern information and media operations on certain corpuses of knowledge. Information and media operations are focused on specific cognitive domains of targeted audience. The effects of so-formed information and communication systems have a direct effect on the organization of individual corpus of (public) knowledge.

This work was supported in part by the Republic of Croatia Ministry of Science, Education and Sports Project ‘Oblikovanje i upravljanje javnim znanjem u informacijskom prostoru’ no. 130-1301799-1999 (project manager: Miroslav Tuđman).

Gordan Akrap is Croatian Government employee (phone: +385 (95) 8027464; e-mail: gakrap@yahoo.de). The views expressed in this paper are a personal opinion of the author and do not represent the views of the institution where author works.

Đilda Pečarić is with the Department of Information and Communication Sciences at the Faculty of Humanities and Social Sciences at The University of Zagreb, Ivana Lučića 3, 10000 Zagreb, Croatia (phone: +385 (0)1 6002320; fax: + 385 (0)1 600 2431; e-mail: dpecaric@ffzg.hr)

## II. Types of Knowledge

Important consequence of the invention and development of the printing industry is the creation of public space and public knowledge. This new space of public knowledge "was never idyllic exchange of knowledge, but rather the space in which are conducted, open wars of text messages" [16]. The aim of these wars was always the same: "to dominate the space of public knowledge in order to conquered (or preserved) the power and authority in society" [16].

There are different divisions of knowledge. In this paper we are interested in models of information strategies and their impact on public knowledge. Therefore, we use division of knowledge into two main groups of knowledge: open and controlled knowledge.

As shown in Figure 1, the first group of knowledge is open knowledge, knowledge that has no access restrictions: public and social knowledge. The second group is controlled knowledge: censored and protected knowledge [16].

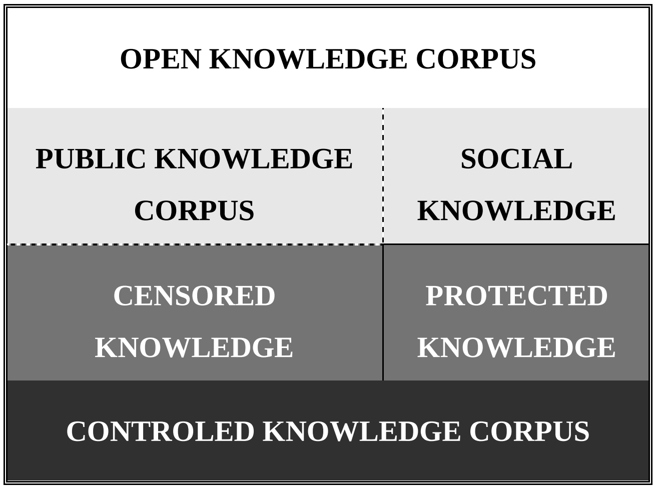

Figure 1**.** Knowledge organization

Corpus of Public knowledge (CPK) is open access knowledge that dominates the public information space. In modern society, public information space is dominated by the public and the mass media, whose functions are presentation, control and supervision of public knowledge, values, ideas and interests that are imposed on society by the domestic and the foreign actors.

Social knowledge is open access knowledge. It includes all social and civilization heritage (traditions, historical and cultural heritage of a nation) which society collects, preserves and shares with other cultures and societies.

Protected knowledge is controlled access knowledge. This is knowledge that an institution, whether it is the state institutions or corporations, have need to protect. Protected knowledge can be "private knowledge (caused by protection of privacy), classified knowledge (different types of secrets), the official knowledge, hidden knowledge, etc." [16].

Censored knowledge is knowledge with controlled access. Since the censored knowledge is the threat to the existing public knowledge, the dominant values, ideas, worldview, etc. they are forbidden by the ruling elite in order to protect their or social interests [16].

Since the boundaries and differences between open and controlled knowledge sometimes are vague and imprecise, therefore the content of certain corpuses of knowledge are neither fixed nor permanent, nor constant. Knowledge gravitate towards constant motion, transition from area of controlled into an area of open knowledge. Knowledge is moving by process that can be called "diffusion of knowledge." To demonstrate the difference in areas among which operates the largest part of the total diffusion, the boundaries among these areas are shown with dotted line while the area of the protected knowledge is bounded by solid line as shown in Figure 1.

Ruling and governing elite strive for total control of process of knowledge diffusion, because in this way they ensure the dominance of their messages as relevant social facts. And therefore they try to "prevent unauthorized penetration into the corpus of controlled knowledge as well as attempt to abandon knowledge from that corpus and their transition into other corpuses of knowledge. At the same time, sometimes, they are trying to protect corpus of open knowledge against penetration and effects of other knowledge which can cause significant changes to the existing paradigm." [1].

## III. Cognitive Hierarchy and Types of Knowledge

The process of knowledge creation is a continuous series of events, the interaction of data from world that surrounds us with the world of information and our cognitive abilities of evaluation and judgment of abstracted reality. Obviously the existence of three distinct domains in relation to the processes of collecting, processing, conversion, storage and interpreting information and decision-making action based upon them, suggests the need for division of the world that surrounds us, and in which we operate, on three different domains: physical world domain, information domain, and cognitive domains [3]. Interaction and synergy of processes conducting in these domains, and through them, enable creation of new useful and applicable knowledge and quality decisions.

The real world domain or the physical domain represents our reality, everyday life that surrounds us, our past and projected, potential and/or the expected version closer and/or further future. Events, symbols and data occur in this domain. We exist and operate at the physical level in that domain.

Information domain is an area in which information exists, in which its creation and distribution within information domain, but also towards other domains is performed. In this domain, the symbols from the world of reality are affected, turning into a form useful for further use and distribution to different users in different, user-friendly manner and forms.

Cognitive domain represents a world of knowledge, world of awareness and perception, a world of intellectual ability and training of individuals, groups and/or community, the domain in which we form the knowledge, create intelligence.

Decisions are made in cognitive domain.

Some authors point out that among the three domains of understanding exist the cognitive hierarchy “another value which is included. The hierarchy includes irrelevant noise too” [5]. Most probably, that “irrelevant noise” which is included in cognitive hierarchy does not allowed easy integration of all three domains of understanding of world.

The condition of a real and effective action of these domains, as well as their content, is the possibility of communication, internal (within each domain separately) and external (among different domains). Properties of the communication channels and means of communication also depends on the efficiency of processing, and distribution of information and the organization of certain types of knowledge [1].

## IV. Information strategies – evolution through time

Process of realizing importance, place and role of information in achieving different aspirations (political, military, economic etc.) leads to changes of approach aspects toward information possibilities. In modern doctrines, information is used as a powerful political, military, economic and diplomatic tool in order to reduce the involvement of the classic military capabilities. The aim of information strategies is to achieve information superiority in the opponent's, and his own, information space.

Information rapidly becomes a target, object and mean of information warfare. Information might become a very powerful and useful weapon in the hands of those who have control of the information and information-communication systems. Those who are able to manage the information model it according to their needs and, using covert methods and tools, spread it through to the opponent's information space, i.e. CPK.

With Information operations (IO), together with Media operations (MO)[1], objectives and tasks defined in the Information Strategies can be fulfilled. The aim is to influence on two key parts of the society, or individual community:

- To the persons who take key political, military, economic and other decisions in order to force them to make decisions in favor of their own damage and
- The associated public opinion in order to encourage their activities against (or to support) the ruling structure, disable their rational actions and encourage mass to seek changes (or to support) in the community, business, society, the state, if necessary, by using violent means and methods.

In different groups, communities, nations or society, information attackers are trying to encourage a sense of fear, insecurity, apathy, hopelessness and lack of confidence in the ruling structure, to encourage target audiences (TA) [2] to act in order to change/support the existing administration. At the same time, influencing the will of TA might stimulate a desire for change and strengthen internal divisions (according the old Roman proverb: divide et impera).

Differences in accessing the subject of IO over time depended on the degree of development of information and communication structures, tools, techniques and technologies as well as depending on the understanding of the importance of information as a means of combat, as shown in Figures 2-4 [2]. On them, it is easy to notice the process of change of models, or adjustment, of IO through time and at the same changes of terminology.

We started to make those figures according to assumption that in the information and communication society, there are three main groups of various publics with associated CPK:

- Domestic public or public at home country of information attackers that ordered/planned and carried out information operations at all levels of the (operational, tactical, strategic) information operations,
- Target Audience in the areas that can be supraregional, regional, national and local nature,
- Other publics that are not part of previously mentioned audiences, and which is not directly connected with them in some form and manner, (political, business, military, social, historical, cultural, religious, ethnic etc.) and
- There are differences in approaches toward domestic and international target audiences.

Modern IO/MO are a permanent in nature. They continue to exist until the completion of the desired goals and tasks. Modern communication systems and resources, especially the Web and developed system of different social networks, represent the new media that can, for a short and long term, affects different TA or to their CPK. They are especially useful in expanding the various (dis)information that publishes "public secrets" in the media, which can influence the public knowledge, shape it and lead to a gradual repositioning of power.

Successfully planned and implemented IO can create conditions in which weaker and technically inferior opponents can, due to achieved information superiority in information space, gain additional benefits that can ultimately lead to their victory. At the same time information and communication system of attackers may become targets of the information attack. Therefore, it is important to protect, especially careful and effectively, their information and communication system.

Therefore, we suggest definition of IO:

> "A set of activities launched toward the enemy information, ICS, persons and cognitive processes with

[1] Media operations have the goal to ensure control over communication channel, in other words, to provide access to and control of desired media.

[2] By definition, the target audience represents objective of the information operations. TA can be one person, small or large group of people and a smaller or larger community.

> the aim of destroying, disabling and slowing enemy activities or to gain control over their activities, while ensuring an adequate level of protection of its own information, ICS, persons and cognitive processes".

To make it very simple: with IO information attacker tries to shape the beliefs and attitudes of an TA, tries to force upon their own will to TA while, at same time, trying to protect same values on their own side. Successfully implemented IO can provide an additional contribution to the strengthening effects of own/allied military forces. Definition of IO shows that information operations can be divided to offensive and defensive information operations. Joint activities of offensive and defensive IO can achieve the best results. It should be noted that the IO does not apply only in times of war. They are subject to continuous activities during time of peace, crisis, war, after the war and during time necessary to re-establish peaceful situation. Although, IO are not used only for political purposes, but they may also make economic damage [4, 11]. Therefore, unreliable knowledge as consequence of IO and MO „can destry results achived utilizing human excellence in product definition“ [10].

Planning and implementation of IO does not belong exclusively to the military and to the intelligence and security services, as it was until the end of the last century. IO are more effective when civilian structures, governmental and non-governmental organizations, companies, institutions and associations are part of this process. IO’s are in function of creating a safe and full (as longer as it can be) information superiority not only in the information space of the opponent, but also in the global information environment (GIE) at all. That is a time-space continuum in which the IO’s are conducted in five existing dimension (3D, time, virtuality-global information network).

### A. *The first stage of planning and conducting IO/MO*

Figure 2 shows the process and methodology of activities aimed at shaping public knowledge in conditions where there is almost no exchange of information between the domestic public and target audience. There is no communication connection between the different publics and their CPK. Moreover, if communication exist, its intensity is very low, which makes the process of sharing information between such publics very weak, almost negligible. Their CPK are separate and do not affect to each other. At the same time CPK of third public, which cannot be regarded as a domestic public or TA, does not have the ability to communicate with other CPK. In such a situation, IO’s that are carried out to attack the opponent's side can be extremely harsh. For achieving the aims of information strategies, information attackers do not refrain to use any possible mean to perform IO’s because there is, virtually, no possibility to discredit their own activities to local public due to poor or no communication between the impact of the target area and the domestic public. As long as the information attacks against TA last, more or less coordinated domestic media operations shapes domestic public knowledge by homogenized it on key issues of national importance.

The objectives of information attackers that have to be achieved against domestic public are very different from the goals that have to achieve against foreign TA. With feedback principle corrections of planned activities can be made. This process, in this first phase has relatively low intensity. Mainly, it is carried out through a network of sources of intelligence and security agencies, and through various forms of activities of specialized military institutions.

### B. *The second stage of planning and conducting IO/MO*

Figure 3 shows the process and methodology of activities in order to form public knowledge in terms of the existence of the exchange of information between different audiences. Conditions that some subversive and aggressive, psychological and special operations expose the public and to reveal publicly their enforcer and their client are created. Client can feel unpleasant situation that it can significantly compromised in front of the domestic and entire international public. Therefore, in process of planning and conducting IO’s becomes necessary to change terminology, approach, methodology, compliance and monitoring the whole process. In order to hide the actual client of IO’s, it is necessary to employ different "mediator" that can serve as an affective cover for implemented IO’s. Those mediators may be different organizations (profit, non-profit, NGO’s), companies (governmental, private, mixed, real, fictional), as well as forms of organized international (supranational, regional and international institutions). Mediators can be located in an area where there is TA. They can be located immediately adjacent to it or may be completely outside of the target area. Different mediators operate toward different audiences, or to different CPK. By employing mediators that are completely outside of the target area, provides an additional level of protection and to the secrecy of information and media operations. Media that operate in the target area are the best mediator in shaping CPK, as well as persons that are part of the top decision-making circles in certain parts of the life of the target audience (political, military, economic, security, media ...).

In addition, because of the possibility of communicating between various audiences, there was a need for closer coordination between domestic and foreign activities of information attacker because of the necessity to prevent possible negative impacts of information and media operations activities abroad to the domestic public.

Since communicology improves existing and develops new communication tools and methods, significant investment in media operations occurs. The aim is to target the audience from selected countries and territories by founding new propaganda radio and TV stations, extending their broadcasting time, extending the number of the foreign language in which they broadcast their program.

Information is gaining a huge importance in shaping public knowledge, but still does not become a strategic weapon. One of the consequences of advanced communication techniques and technologies in a new, information era is a possibility of a stronger impact to the process from information provided by the feedback connection. Comparing the effectiveness of those operations is necessary in order to be adapted to new challenges and new situations while monitoring the effect of IO and MO against TA.

### *C. The third stage of planning and conducting IO/MO*

Figure 4 shows the process and methodology of activities in order to form public knowledge in the GIE. Complete, global, connectivity virtually by all available (important) audiences that may affect the process of shaping public knowledge exist. Without significant amount of risk, it is no longer possible, even using covert operations, to run IO'a and MO's against a TA because of the risk of their recognition by the TA and discrediting the operations toward domestic public.

Therefore, it is necessary to find new ways and methodologies to increase the efficiency of implemented operations, to make more difficult to make identification of the information client, planners and implementers possible. The model shown in Figure 3 is further modeled by the introduction of new intermediaries in the form of various "independent government" institutions, non-governmental and non-profit associations and organizations and by inter-relation with the mainstream media. By planning and implementation of long-term activity, full control over the process of collecting and information processing can be achieved. The main role in those activities has associations and organizations operating near TA. They can achieve the greatest effects with minimal investment and minimal risk of being compromised.

On the other hand, the integration of various audiences and public knowledge, impose the need for a much higher level of integration and coordination of activities of IO's planners and implementers. Politically correct terminology such as spin-doctors, opinion makers, image-makers, public diplomacy and strategic communication, perception management is introduced.

Due to the increasing integration between state and private interests, there is a need to protect the interests of big business by government institutions. The result is linking their efforts to different forms of public-private partnerships in the establishment of various trusts and/or institutions which then can encouraged, financed, supported, organized and implemented the processes of change the opinions, attitudes and perceptions of TA.

Various non-governmental, non-profit and "independent" organizations that are supported by the national government, serves the interests of those same governments, but openly and covertly, acts on information collection, dissemination and distribution processes, about and against the TA. At the same time, while working towards the targeted audiences, they collect data and information that are used for intelligence and security purposes. However, unlike previous cases, these organizations and associations also serve to collect data and information on public reactions and exposure of TA to IO/MO thus enabling more efficient adaptation/change of the default settings of the IO plan in accordance with new situations. Alternatively, we can say that they are almost perfect part of the feedback control process.

With the globalization of information and communication systems, a new doctrine that is trying to avoid conflicts or generate them, depending on the information attacker needs and plans appears. The doctrine of Low intensity conflicts (LIC) in which information (and its derivatives) in the whole range of activities, plays a key role in order to fulfill the ultimate goal of every national information strategy (NIS): the creation of the Global Information Superiority (GIS).

Nowadays, LIC becomes the dominant form and way of dealing with international and local threats. The articulation of national information strategies should ensure political, economic, cultural and military domination of the actors on the global scene. National, as well as business, information doctrines and strategies define offensive and defensive methods and techniques of usage of information resources with aim to ensure information superiority. New national strategies are based on the requirement to achieve information superiority on all levels (local, national, regional, global).

A characteristic feature of this way of conducting IO is the fact that the cognitive domain has become the primary battleground, information domains secondary and physical domain the last.

By system shown in Figure 4 information becomes a fully strategic power, fourth instrument on which, in addition to diplomatic, military and economic, sovereign state/institutions/companies can based their power/influence. NIS is the foundation for managing global expansionist policies at local and regional levels of implementation. Information and media operations have become the main "modus operandi" in implementing such policies.

This system has provided strong feedback (due to the possible existence of a large number of high-quality data obtained from independent sources) that allows:

- Monitoring the implementation of planned and initiated activities,
- Fast and efficient reaction with a view to (re)shaping of individual activities at the strategic and tactical level according to the collected data and information and
- Preparation of periodic and final reports with suggestions to improve future actions.

In this phase however, the collection of information through a process of feedback, should be especially careful because there is always the possibility of oversupply in the recipient's information system that can significantly slow down the system and making it much less effective (an information overload). At the same time, there is the possibility that attacked TA deliberately send misinformation and disinformation if attacked TA recognizes some form or methodology by which they will realize that they are exposed to the IO/MO.

The process shown in Figure 5 allows the planning and implementation of highly effective methods, so called "information laundry" that an make a strong impact to targeted public knowledge and to the key decision-makers (political, military, economic, security, social…). That means that, in a first phase, information attacker send an desirable information content that has to influence TA through other, „independent“ and „far enough“ communication channels. In a second phase, this content has to be carried out to the TA by communication channel that is under information attacker (in)direct control. After the desired information content has been published, information attacker, or someone else, is able to base their activities, based on published information by “independent and reliable” sources.

## V. Information-communication Systems and Information Superiority

The development of information and communication technologies (ICT) has created the conditions for a quick and efficient use of data and information in many areas of human activity and also the development of new doctrine that old, hegemonic, goals are trying to achieve by applying new methods and means. Although it has been known for a long time that the value of possession and usage of the right information at the right time and in the right way, just the modern information and the ICT age allows their full usage as deadly, non-kinetic, resources that is used in the process of imposing one's will to different target audiences. Armed aggression is replaced by informational aggression. Superiority in the human military force is replaced by superiority of experts for public relations and media workers. Superiority in weapons and lethal means is replaced by the superiority in the information and technical and technological development. Superiority in controlling and monitoring of the battlefield turned into a superiority and control of the media space. Battlefield is no longer dependent on space and time. Battlefields are media, and ICT space in which different IO/MO can last for 24 hours a day, 7 days a week, 12 months a year.

Therefore, in the opponent, (in this case primarily informational) environment, with the aim of preventing the organization of an effective defense, do not any more send commandos and saboteurs, but people that works undercover, for example, various NGOs, operates towards a TA in line with the aspirations of the information attacker. Information commandos/saboteurs generally used method of "information laundry" to shape corpus of public knowledge of TA in the programmed direction. One of their priority tasks is disabling defense activities of TA that can lead to recognition of offensive actions the processes that shape its CPK and the fact that it has become the subject of IO/MO. If TA is not able to recognize that is under the exposure of the information attacker, it will not be able to organize successful defense and its CPK is going to be designed and operated in accordance with the information attacker's intentions.

Creation of monopoly over the process (one, several or all together) of the collection, processing, storage, interpretation, usage of data, information and knowledge is objective of information strategies that has direct influence of the information attacker on the available corpuses of knowledge of target audience.

The impact on existing contents of knowledge can be done in several ways:

- Changing,
- Deleting,
- Neglecting and
- Creating new content in accordance with the interests of the information attacker.

Corpuses of knowledge that are the objectives of the information attacker are subject of information and communication system (ICS) processing shown in Figure 5. ICS represents process by which external input values (data and information) using technical and technological tools and the human mind, convert intelligence, as a base for making the necessary quality, effective and timely decisions into knowledge. Process presented here shows the complexity and interdependence of system’s internal link whose efficiency depends on:

- The content of the information that passes through the ICS,
- Persons involved in the creation of new values,
- Technical and technological solutions that enable more efficient operation and
- The time required to process input values in order to receive final and usable output value, decision.

Input values of this system are collected from outside, mainly from physical domain. Part of the input values comes from the information domain. The first step in the process represents the process of verification of accuracy and completeness of input values, reliability control of the sources of input data is carried out, and its comparison with the existing content in the corpus of its own knowledge.

Output product of the first phase is the information, which is, in the second phase, compared with the other information that exist in the information domain. In the second phase, information is going under the process of verification of authenticity and interpretation that gives the output value: knowledge. In the third process in this ICS, created knowledge is undergoing a process of comparison with the default values: pre-planned objectives and tasks of the management process. Last output value is intelligence on which decision of activity is based upon, which in turn has a (certain) consequences on the physical domain of reality and on the changes in the organization and content of certain corpus of knowledge. Corpuses of knowledge are not dead and static systems because the ICS function is to serve as a feedback loop for the correction of the output values of certain cognitive stages. In other words, one of the tasks of ICS is to try to enable early detection of information activity of the information attacker.

The goal of the information attacker is to take a control over the content of certain corpuses of knowledge, and therefore ICS, either in parts or in whole. As it is evident from Figure 5, the influence on the available corpuses of knowledge is carried out in all available individual processes within the ICS. Through the process of verification and control of inputs, establishment of credibility and interpretation and the planning and management of certain processes, directly affects the available corpuses of knowledge.

If however, for some reasons, the information attacker is not successful in process of undertaking the control of ICS and its content, an information attacker may encumber the corpus of available knowledge of the TA by numerous informational contents and bring it into a state of information overload. In such a situation it is significantly aggravated effectiveness of ICS because TA is smothering by useless values, TA actions are slowing down. Information overload generate informative chaos that aggravates rational decisions.

## VI. Possible Effects on the Corpus of Public Knowledge

The application of information and media operations based on the NIS, is not and cannot always be successful. There are a corpuses of knowledge (such as protected knowledge in Figure 1), which are difficult to access and difficult to shape in accordance with the aspirations of the information attackers. Effectiveness of the planning and implementation of IO/MO depends on successful development of several important values:

- The availability of different media,
- Freedom and quality of the media,
- Perception of the current reality of TA and
- The organization of society.

In order to make necessary changes and influence the TA using IO/MO, several important determinants must be met: (numerous) media[3] must be available, social system must be open, and there should exist a part of the population that is (more or less) dissatisfied with the status quo and ready to make changes.

On the other hand, there are situations that information attacker, while conducting IO/MO is trying to keep the status quo. In those situations, IO/MO has an advantage in the process of imposing the will of information attacker over military operations.

Control of the media world is one of the key conditions for achieving information superiority as it can simultaneously monitor both communication channel and content that passes through. In restricted, totalitarian, societies where the media are poorly or not available, with complete control of the media world, it is very difficult to make a decisive impact on the corpuses of knowledge of TA, even after long-term operations. Information attacker in such situations is focused on the usage of other (intelligence services and/or military force) methods of activities in order to achieve the conditions for the effective execution of the objectives.

Between these extremes there are situations where it might be that with combined effects of kinetic and non-kinetic resources in the process of imposing one's will to certain TA.

Differences of TA[4], given their numerousness and level of possible impact on the decision-making process, conditioning and different approach to the process of imposing one's will.

According to small groups of people, especially those who can make important decisions, that is clearly and unambiguously influence in accordance with the wishes of the information attackers, most often are applied methods and means that are used by intelligence-security systems. For efficient operation of the more numerous TA, are used information and media operations as shown in Figure 6. Taking the control over information and communication systems and contents that passes through creates the conditions for achieving information superiority and imposing one's will to a TA.

In the initial part of the curve from Figure 6, which includes influential individuals and small groups (those who make decisions, participate in making decisions, or may significantly affect the decision-making in which should definitely be involved, leading journalists and columnists in the most influential media) dominated activity are run by intelligence and security agencies that have a goal, by using distinctive methods, practices and tools, to prepossess these individuals to achieve their own interests.

IO/MO against the other TA shall apply with the aim of controlling the content that to certain TA is exposed to, as well as control and surveillance of communications facilities (media) by which the stated content is displayed. Namely, management of activity of larger groups or communities can directly influence on decision-making as shown by dashed (-..) lines.

## VII. Conclusion

Taking control of ICS is a primary condition for achieving information superiority and imposing one's will to the target audience. However, the effects of information operations are not limited to the attacked, target audience and its corpuses of knowledge. Due to the existence of global information environment, consequences of IO on any target audience can influence knowledge corpuses of information attackers. Therefore, without significant amount of risk it is no longer possible, even in a disguised way, to run IO against a selected TA because of the risk of their recognition by the TA and because of the mirrored side effects in their own society.

Information attackers are investing significant resources (financial, technical, technological, human, and time) in the processes and actions that attempt to gain information

[3] Particularly those media that have non-transparent ownership.

[4] Target audiences are different also by other numerous characteristics. Some of them are sex, race, religion, culture, tradition and education. Here, we take into account the distribution on numerousness and level of influence on decision-making of the general importance.

superiority with the help of information and media operations. These operations are now the dominant forms of conflicts when TA might not be aware that is under attack. These operations are trying to impose the information attackers will to TA, reshape the corresponding body of public knowledge in accordance with their own needs, to create the conditions under which the TA future will be designed to achieve the goals of information attacker and the conditions when the TA makes decisions in accordance with the aspirations of the information attacker.

The development of modern information and communication technologies and resources enable the further development of the information doctrine that the old, hegemonic aims, are trying to be fulfilled by the application of new methods and tools.

The existence of a numerous of IO that mutually confront to each other is reality which last and it will last. Because effects of implemented IO can be turn against information attacker as well, they have to look for new methods to conceal their activities.

True, truthful, and objective informing is no longer the primary goal of the mass media. Therefore, the knowledge, especially knowledge of the public corpus, is exposed to many information attacks. Unlike the weapons of mass destruction, the mass media have become a tool for the implementation of cognitive operations (M2CO - Mass Media Cognitive Operations). This is especially fact for the media that exist in the virtual world because:

- Of the velocity of publication, change, and the availability of published (dis)information,
- A possibility of interaction between recipient and content and
- Ability to conceal the authorship on the placed (dis)information that lead to the behaviours and actions in the virtual world that causes serious consequences in the real world.

Media managed by information attackers creates the perception of TA by the relativization of history, their decontextualization and new recontextualization, transformation of memories in order to achieve the projected future as the individuals, groups, communities and nations. Such media simplify to the end system of traditional and moral values that underpin community trying to impose a new ideology of consumerism, nihilism, hedonism, materialism, non-patriotism, transience and simultaneously promotes the culture of fear, insecurity, and vindictiveness with imposing many prejudices.

Since the war has also defined rules by which it can be lead, we believe that is necessary to try to define the rules for the implementation of information and media operations. It is necessary to encourage research in order to determine facts, truth based on real facts, prevent media monopolies of information distribution, and to insist on responsibility for publicly said or published words/expressions which encourages any form of hatred, violence, segregation. It is necessary to encourage the publication of truthful, ethical, objective and complete information, to respect and promote the common good as well as the system of moral values, respect the dignity of individuals, families and communities, to encourage optimism, respect differences and to establish an educational system that will encourage a true and objective deliberation, action and research, and not monotonous learning without understanding.

A special "contribution" to successful IO/MO is given by today's technical and technological solutions that have the raised ability to communicate to previously unknown levels. Those solutions might, to the TA that can be by using traditional forms of warfare easily loose any battle and war help them to preserve themselves from information attackers, and even win if they are able to reach superiority in information and cognitive domain.

Individuals and groups can use the Web opportunities to promote their views and needs with significantly less investment (money, people and time) than the governments and corporations must do. In other words, the Web has created the conditions under which asymmetric conflicts are gaining new meanings, power centers can be moved from the existing to the new centers in accordance with the diffusion of knowledge, while the gravity action focus is moved to the cognitive domain.

News in the media are not published by accident. Content of the published news today is just an interpretation of events in accordance with the policies governed by interested individuals or groups. Although sometimes the published news are trying to be presented as a product of mere coincidence, many of the information, especially those that are on the magazine covers that sells media, in most cases are product of targeted activities towards a specific TA. However, it should be noted that the public knowledge is formed not only target by publishing some content. It is shaped also in a process of not releasing certain content that, at that moment or period of time, do not match (for various reasons) the editorial policy, or aims of the informational attacker.

Without significant amount of risk it is no longer possible, even in covert ways, to run IO/MO against a TA because of the risk of their recognition by the TA and discredit the information attacker by its domestic TA. Therefore, it is necessary to find new ways, methods, and methodologies to increase the concealment of planed and implemented IO to make it more difficult that the client, planners and implementers of IO/MO can be identified.

Every medal has two sides. But there are facts that broad consensus should accepted as an integral part of the corpus of public knowledge. By their recognition and existence, those facts can prevent the negative effects of IO/MO, in order to thwart attempts by deforming the truth, manufacturing consent to a different future.

We want to point it very clearly that, especially today, information doctrines and strategies are necessity that should exist. That means that it should be known how to implement them, in order to organize a modern society that aspires to the rapid and efficient development to stable society (as well as businesses, research institutions ...). If an entity does not have a clearly defined national strategy, including information, defensive ability against different types of attacks, as well as from different attackers, reduced considerably. In addition, the fact that attacked might not even be aware that is the target of information attack.

IO/MO does not happen to someone else. Today everyone can be exposed to IO/MO because none of them is not sufficiently immune to their effects, and at a certain stage and at a certain level, fails to produce (for the attacker) side effects. Attacked entities must be able to rise up the necessary questions:

- Can we recognize when we are exposed to IO attack?
- Can we figure out what is the real reason for starting these IO?
- Who is behind them?
- Can we prepare countermeasures and whether we can successfully implement them?

If there are some negative answers to these questions, information attacker has a significant chance to realize his plan while TA has no possibility of organizing an effective defence.

Armed conflict or war is not prohibited by international law as a way of solving problems. However, the Geneva Conventions and other international legal acts, defined some principles that must be met and respected in the conduct of war. Therefore we consider it necessary to establish a code of conduct in the realization of information strategies to individual TA (foreign and domestic) at the international level. At the same time it is necessary to standardize the criteria according which is going to be able to evaluate negative content (false facts; misinformation, disinformation) that can be found in certain CPK, to be able to remove them from it. That would enable stable, and significantly less disturbed, society development on national and international level.

## REFERENCES

[1] G. Akrap, “Informacijske strategije i oblikovanje javnoga znanja,” *National security and the future*, vol. 10, no. 2, pp. 77 – 151, 2009.

[2] G. Akrap, “Informacijske strategije i operacije u oblikovanju javnog znanja,” Ph.D. dissertation, Odsjek za informacijske I komunikacijske znanosti, Filozofski fakultet, Sveučilište u Zagrebu, Zagreb, 2011.

[3] D. S. Alberts, J. J. Gartska, R. E. Hayes, D. A. Signori. (2001). Understanding Information Age Warfare. Available: http://www.dodccrp.org/files/Alberts_UIAW.pdf (22.4.2010).

[4] I. Bernik. Information Warfare Effects on Businesses in Slovenia// Recent Advances in Information Science. Proceedings of the 7th European Computing Conference. Recent Advances in Computer Engineering Series. WSEAS Press, 2013, pp. 42-47.

[5] Z. Bradac, M. Sir, V. Kacymarcyzk, I. Vesel. Knowledge and Data Fusion. Recent Researches In Communications And Computers. Kos Island (CSCC ‘12. WSEAS Press, 2012, pp. 63-67.

[6] R. Cappurro. (2000). What is Angeletics?. Available: http://www.capurro.de/angeletics.html, (9.09.2013).

[7] R. Cappurro. (2006). Knowledge Map of Information Science. Available: http://www.capurro.de/zins.html, (9.09.2013).

[8] R. Cappurro. (2012). Ethics and Public Policy within a Digital Environment. Available: http://www.capurro.de/ethicomp02.html, (9.09.2013).

[9] *Department of the Army: The United States Army's: Cyberspace Operations Concept Capability Plan 2016-2028*, TRADOC Pamphlet, 2010, pp. 525-7-8,

[10] L. Horvath, I. J. Rudas. New Method of Knowledge Representation and Communication for Product Object Modeling. Latest Advances in Information Scence and Applications. WSEAS Press, 2012, pp. 75-80.

[11] P. Hruza, A. Chlan, R. Sousek. Cyber Attacks and Cyber Warfares. Recent Researches in Telecommunications, Informatics, Electronics and Signal Processing. Recent Advances in Electrical Engineering Series. WSEAS Press, 2013, pp. 100-107.

[12] T. Saracevic, “Relevance: a Review of and the Framework for the Thinking on the Notion of Information Science,” *Journal of the American Society for Information Science*, vol. 6, no. 26, pp. 321-343, 1975.

[13] B. Težak, “Uvod,” *Informatologia Yugoslavia*, vol. 1, pp. 1-4, 1969.

[14] B. Težak, “Informaciono-dokumentaciono-komunikacioni (INDOK) sistem. Emisionotransmisiono – akumulaciono –selekciono - apsorpcioni (e-t-ak-s-a) kompleks kao konceptualna podloga INDOK-sistema,” *Informatologia Yugoslavia*, vol. 1, no. 1-4, pp. 1-11, 1969.

[15] B. Težak, “Informacione znanosti i službe: njihova struktura, odnosi i politika”, *Informatologia Yugoslavia*, vol. 1, no. 1-4, pp. 13-30, 1969.

[16] M. Tuđman, *Informacijsko ratište i informacijska znanost*. Hrvatska sveučilišna naklada, 2008.

[17] M. Tuđman, *Prikazalište znanja*. Hrvatska sveučilišna naklada, 2003.

[18] *USA Joint Chiefs of Staff, Joint Pub 3-13: Information Operations*, 2006, Available: http://www.marines.mil/unit/mcioc/Documents/Joint%20IO%20JP3-13.pdf (10.9.2010).

[19] *USA Joint Chiefs of Staff, Joint Pub 3-13.2: Psychological Operations*, 2010, Available: http://www.dtic.mil/doctrine/new_pubs/jp3_13_2.pdf (5.2.2010).

[20] J. Ziman, *Public Knowledge: The Social Dimension of Science*, Cambridge University Press, 1968.

**Gordan Akrap** received his doctorate degree in 2011 in the field of Information Science at University of Zagreb, in Zagreb, Croatia. The author’s major fields of study are Information strategies and Influence operations especially during Croatia’s Homeland war.

He was active member of Croatian security and diplomatic structures during and after the Croatian Homeland war for what he had received several medals. Also, he finished Croatian Diplomatic academy and numerous courses with intelligence and security background.

He is an author and co-author of four books and several articles about intelligence and security history and public knowledge influence in journals with international editorials.

He is a member of International Intelligence History Association and member of editorial staff in a National Security and Future Journal.

**Đilda Pečarić** received her doctorate degree in 2010 in the field of Information Science at University of Zagreb, in Zagreb, Croatia. The author’s major field of study is Bibliometric.

From 2006 she works as teaching assistant at the Department of Information and Communication Sciences, at the Faculty of Humanities and Social Sciences at University of Zagreb, Zagreb, Croatia. From 2011 she works as senior teaching assistant at the Department of Information and Communication Sciences, at the Faculty of Humanities and Social Sciences at University of Zagreb, Zagreb, Croatia. Previous publications are: Đilda Pečarić. Development of Information Sciences in Croatia. Bibliometric Analysis of Doctoral Dissertations in Information Sciences from 1978 to 2009. Saarbrücken: LAP LAMBERT Academic Publishing, 2011.; Miroslav Tuđman, Đilda Pečarić. “Prilozi dubinskoj analizi komunikacijskih obrazaca,” Informatologija 42, 2(2009), pp. 87-92.; Đilda Pečarić, Miroslav Tuđman. “Theoretical difference between impact factor and influence factor” JIOS 34, 1(2010), pp. 133-140. Her field of interest is Bibliometric, Graphical presentation of data, Teaching Methods and Education.

## APPENDIX

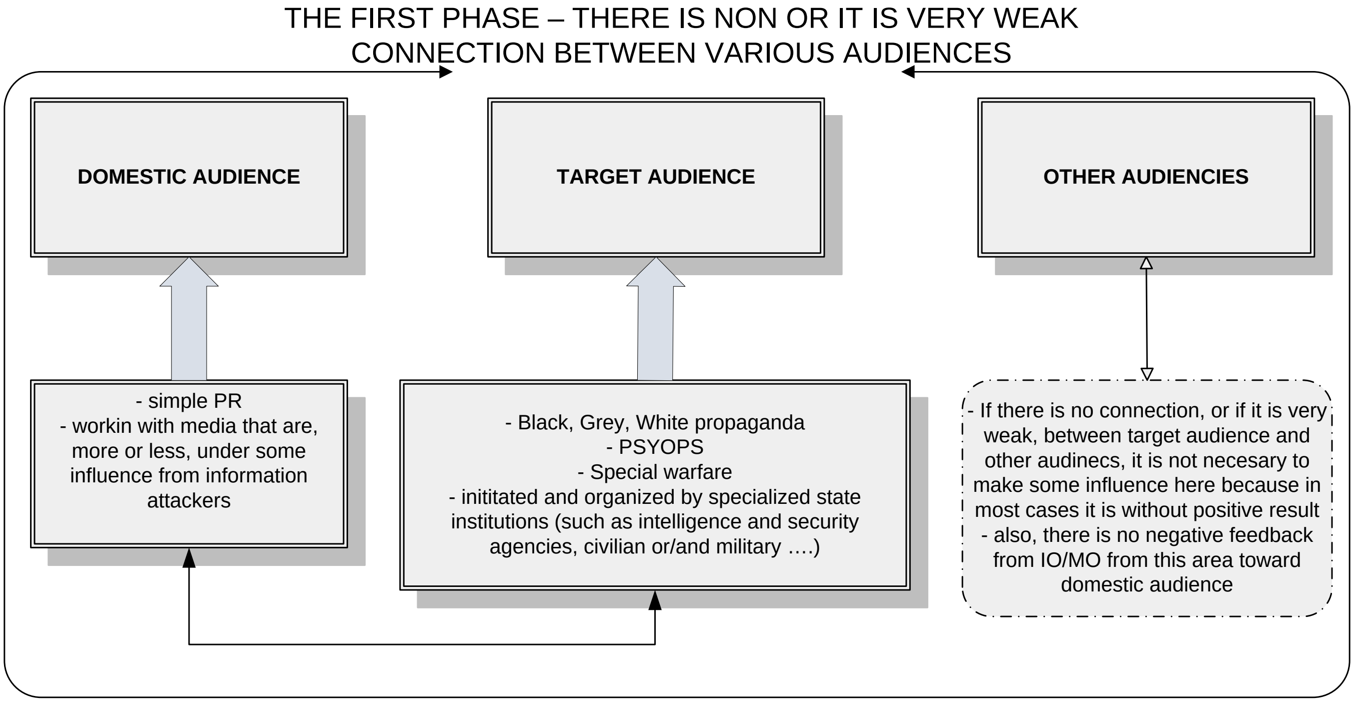
THE FIRST PHASE – THERE IS NON OR IT IS VERY WEAK CONNECTION BETWEEN VARIOUS AUDIENCES
DOMESTIC AUDIENCE
TARGET AUDIENCE
OTHER AUDIENCIES
- simple PR
- workin with media that are, more or less, under some influence from information attackers
- Black, Grey, White propaganda
- PSYOPS
- Special warfare
- inititated and organized by specialized state institutions (such as intelligence and security agencies, civilian or/and military ….)
- If there is no connection, or if it is very weak, between target audience and other audinecs, it is not necesary to make some influence here because in most cases it is without positive result
- also, there is no negative feedback from IO/MO from this area toward domestic audience

**Figure 2.** First phase of IO/MO

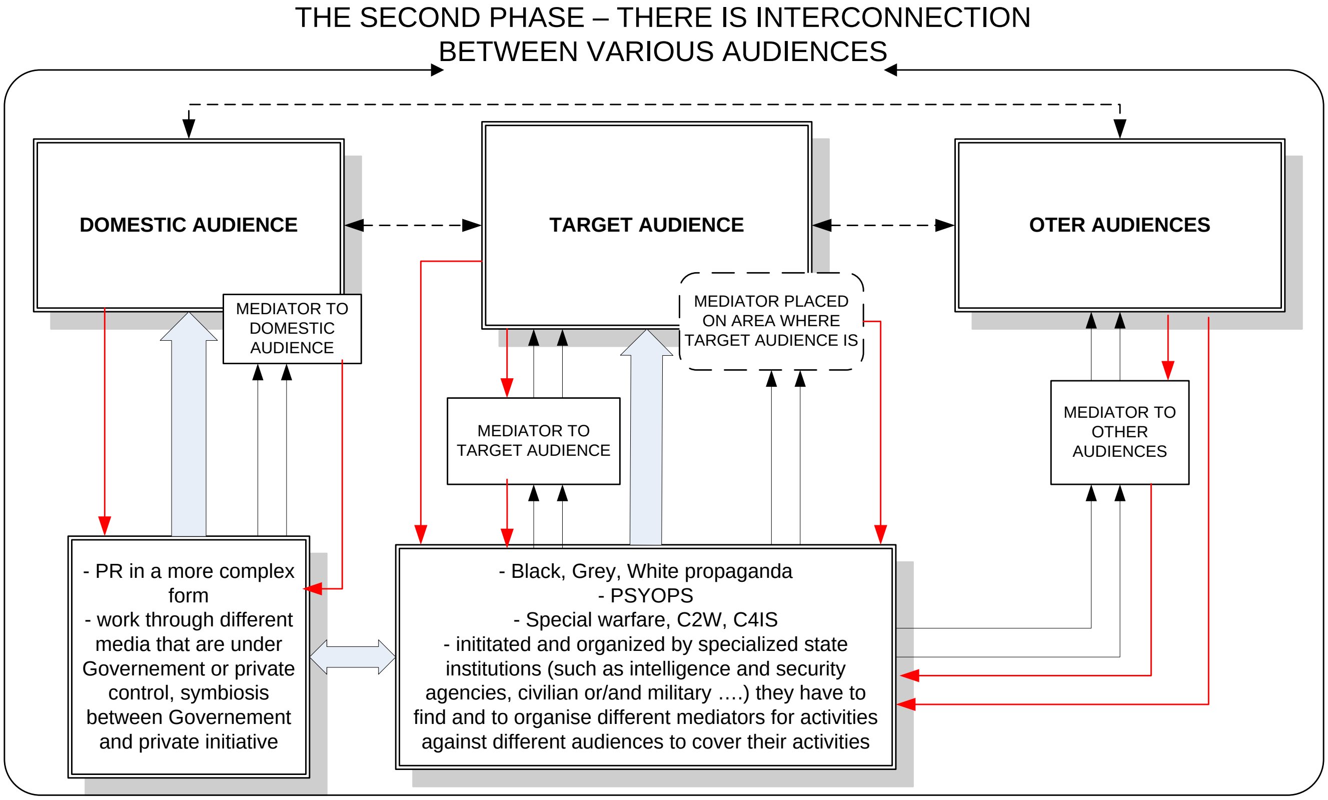
THE SECOND PHASE – THERE IS INTERCONNECTION BETWEEN VARIOUS AUDIENCES
DOMESTIC AUDIENCE
TARGET AUDIENCE
OTER AUDIENCES
MEDIATOR TO DOMESTIC AUDIENCE
MEDIATOR PLACED ON AREA WHERE TARGET AUDIENCE IS
MEDIATOR TO TARGET AUDIENCE
MEDIATOR TO OTHER AUDIENCES
- PR in a more complex form
- work through different media that are under Governement or private control, symbiosis between Governement and private initiative
- Black, Grey, White propaganda
- PSYOPS
- Special warfare, C2W, C4IS
- inititated and organized by specialized state institutions (such as intelligence and security agencies, civilian or/and military ….) they have to find and to organise different mediators for activities against different audiences to cover their activities

**Figure 3.** Second phase of IO/MO

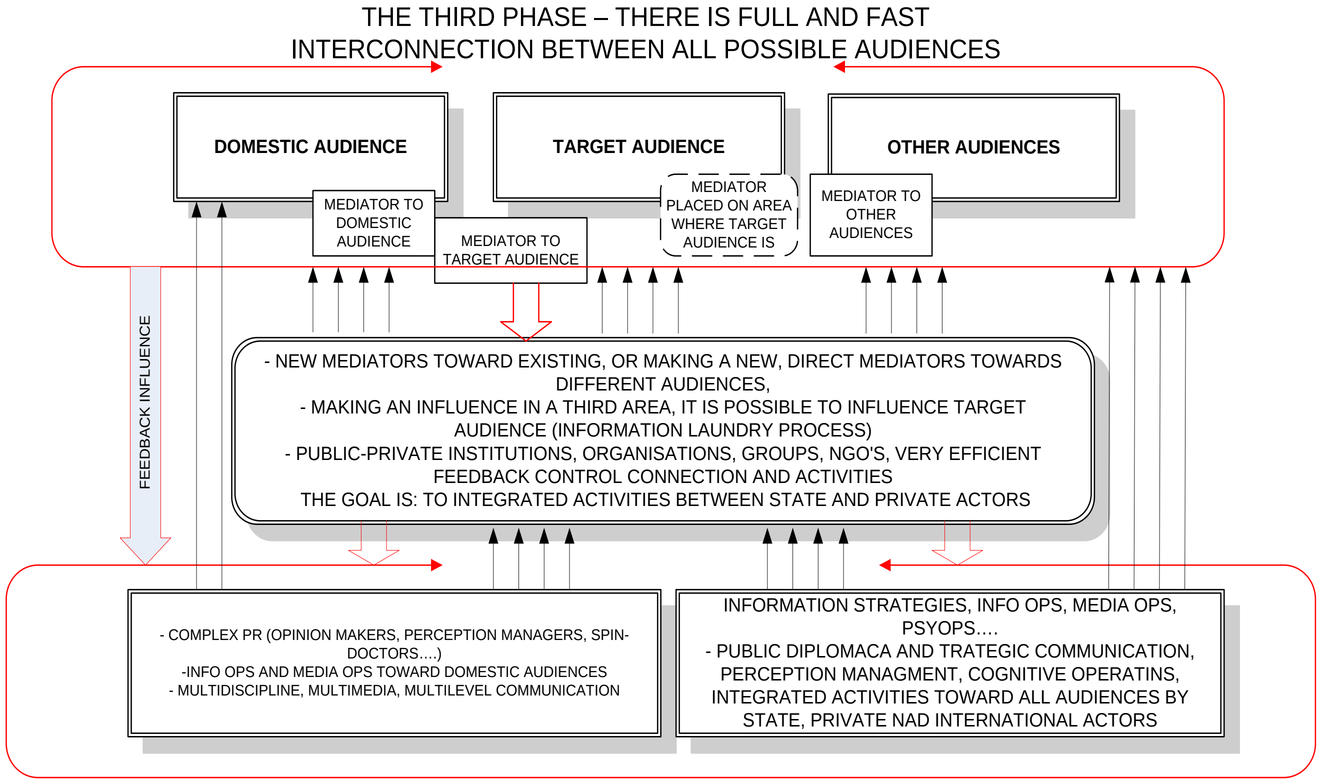
THE THIRD PHASE – THERE IS FULL AND FAST INTERCONNECTION BETWEEN ALL POSSIBLE AUDIENCES
DOMESTIC AUDIENCE
TARGET AUDIENCE
OTHER AUDIENCES
MEDIATOR TO DOMESTIC AUDIENCE
MEDIATOR TO TARGET AUDIENCE
MEDIATOR PLACED ON AREA WHERE TARGET AUDIENCE IS
MEDIATOR TO OTHER AUDIENCES
FEEDBACK INFLUENCE
- NEW MEDIATORS TOWARD EXISTING, OR MAKING A NEW, DIRECT MEDIATORS TOWARDS DIFFERENT AUDIENCES,
- MAKING AN INFLUENCE IN A THIRD AREA, IT IS POSSIBLE TO INFLUENCE TARGET AUDIENCE (INFORMATION LAUNDRY PROCESS)
- PUBLIC-PRIVATE INSTITUTIONS, ORGANISATIONS, GROUPS, NGO'S, VERY EFFICIENT FEEDBACK CONTROL CONNECTION AND ACTIVITIES
THE GOAL IS: TO INTEGRATED ACTIVITIES BETWEEN STATE AND PRIVATE ACTORS
- COMPLEX PR (OPINION MAKERS, PERCEPTION MANAGERS, SPIN-DOCTORS....)
-INFO OPS AND MEDIA OPS TOWARD DOMESTIC AUDIENCES
- MULTIDISCIPLINE, MULTIMEDIA, MULTILEVEL COMMUNICATION
INFORMATION STRATEGIES, INFO OPS, MEDIA OPS, PSYOPS....
- PUBLIC DIPLOMACA AND TRATEGIC COMMUNICATION, PERCEPTION MANAGMENT, COGNITIVE OPERATINS, INTEGRATED ACTIVITIES TOWARD ALL AUDIENCES BY STATE, PRIVATE NAD INTERNATIONAL ACTORS

**Figure 4.** Third phase of IO/MO

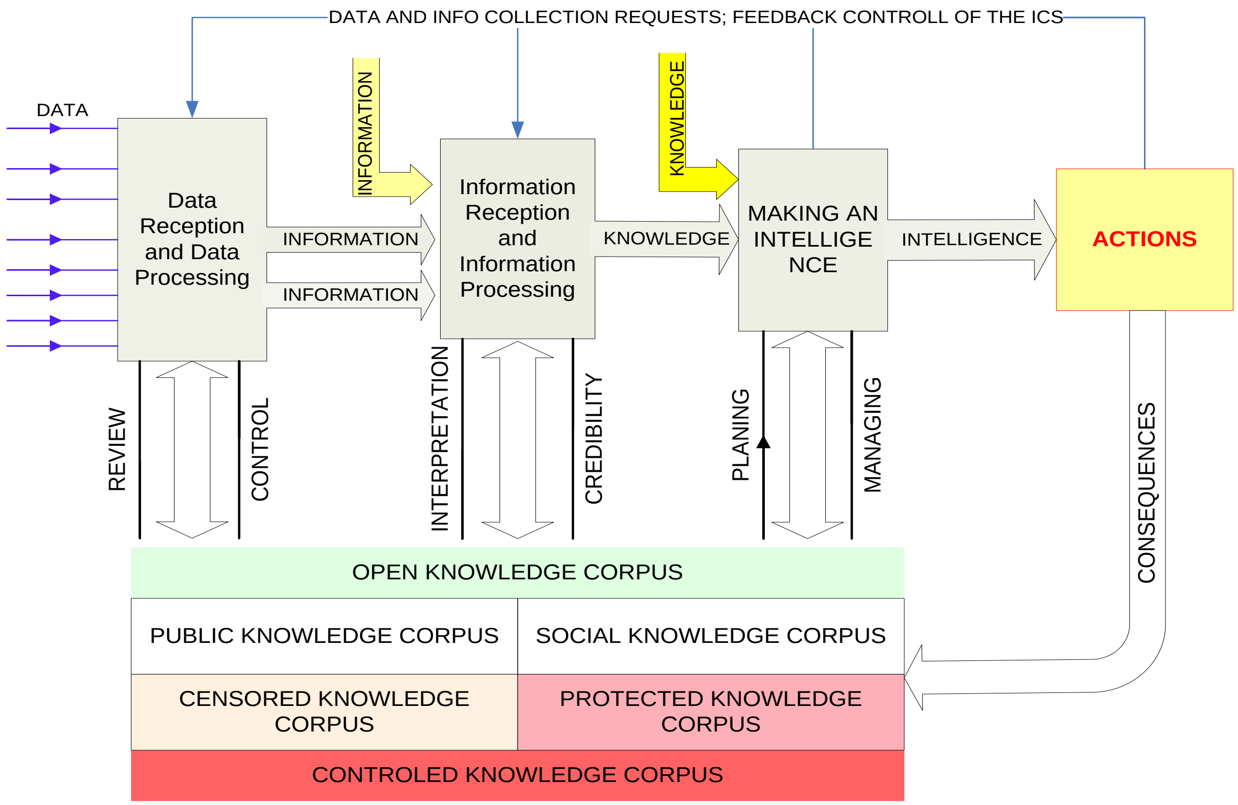

**Figure 5.** Information and Communication System

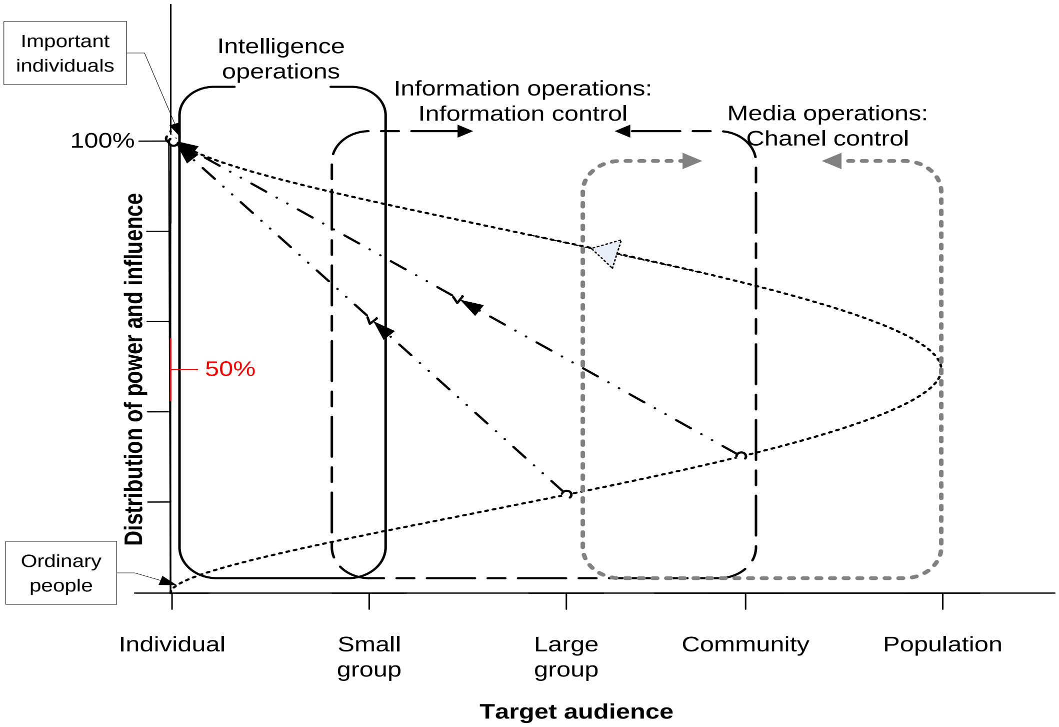

**Figure 6.** Display different modes of action toward different TA’s