The European Proceedings of
Social & Behavioural Sciences
EpSBS

ISSN: 2357-1330

https://doi.org/10.15405/epsbs.2019.12.04.286

SCTCMG 2019

International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism»

INFORMATION WARFARE TECHNOLOGIES AND PSYCHOLOGICAL OPERATIONS WITHIN INTERNATIONAL RELATIONS AND WORLD POLITICS

Andrei Manoilo (a)*, Alla Borisova (b), Vladislav Telichko (c), Anatoliy Petrenko (d)
*Corresponding author

(a) Lomonosov Moscow State University, 27 B, Lomonosovsky Ave., Office G-638, Moscow, 119992, Russia
cyberhurricane@yandex.ru, 7 (926) 7770002
(b) Lomonosov Moscow State University, 27 B, Lomonosovsky Ave., Office G-638, Moscow, 119992, Russia
alla.borisov2011@yandex.ru, 7 (968) 7163468
(c) Russian Presidential Academy of National Economy and Public Administration,
84, Vernadsky Ave., Moscow, Russia, telich.v@mail.ru, 7 (916) 1968514
(d) Lomonosov Moscow State University, 1, Sparrow Hills, Moscow, 119992, Russia
aipetr@rambler.ru, 7 (916) 1425587

Abstract

The paper is devoted to the study of information warfare technologies in modern international relations and world politics. The author notes that in modern conditions the information warfare became a tradition for the surrounding reality. Each of us almost every day finds himself under the influence of any information attack causing terrible aggression aimed at both the society in general and the consciousness of each person separately. The information warfare technologies based on manipulative control of political consciousness and behavior of citizens are exclusively dangerous and are never directed to creation: their main task is to split and polarize the society, to tear it to pieces and fragments, to make these fragments truly hate each other thus causing confrontation with further fight for destruction, or to unite their aggression into a single flow against authorities in power. Thus, the main objective of the information warfare is to break the will of the opponent to resistance and to subject his consciousness to such will. Besides, the majority of the most dangerous operations of American information warfare are based on the same standard organizational scheme representing the sequence of information attacks divided by exposition periods (information silence) and coordinated by time, purposes, tasks and targets. The information warfare technologies are actively and widely applied not only in western countries (mainly the USA where the term "information warfare" is formally stipulated in the U.S. Army field manual *Psychological Operations*), but also by international terrorist organizations and groups.

Keywords: Policy, international relations, information warfare, psychological operations, security.

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The Information Warfare (IW) is an armed conflict where clashes between the parties take place in the form of information operations and with the use of information weapons.

Structurally the modern information warfare includes the sequence of information operations united by a single plan and coordinated by purposes, tasks, forms and methods of information influence.

Mass communication media plays a special role in modern information warfare. On the one hand, serves the information channel for specific target audience (political elite, opinion leaders, general public, politically active youth) and on the other hand, it acts as a direct participant of conflict interaction. In modern conflicts, the media is actively used as means of misinformation and promotion, as a tool of manipulation of public opinion, mass consciousness and behavior of citizens, and as a tool of direct pressure upon opponents. The so-called "independent" media helps the intelligence agencies to perform attacks ("controlled leaks") of information compromising rivals, destabilizing political situation in various countries, initiating color revolution-style massive protests.

2. Problem Statement

In the United States, the term "information operation" is formalized in combat documents. From 2007 to 2010 almost all actions were called "psychological operations" (FM 3-05.301 "Psychological Operations Process Tactics, Techniques, and Procedures" (DTIC, 2007)). Now psychological operations form the general system of information operations. The main regulatory documents of operations, tactics, techniques, and procedures in this field include JP 3-13 "Information Operations"; JP 3-61 "Public Affairs"; FM 3-13 "Information Operations"; FM 3-53 "Military Information Support Operations" (DTIC, 2013); FM 3-61 "Public Affairs Operations" (FAS, 2014) and some other official documents of the U.S. Army (FAS, 1988; FAS, 2014; DTIC, 2005; DTIC, 2010; DTIC, 2006; DTIC, 2011). According to these sources, the information operation is a planned propaganda and psychological activity in peace or wartime aimed at foreign friendly, hostile or neutral audience in order to influence its attitude and behavior to achieve favorable political and military goals. At the same time, the US military identify three levels of information warfare: strategic, tactical and operational. The tactical level of information warfare covers single information attacks (IA). The operational level includes a set of information attacks performed following integrated information operations. The strategic level corresponds to the information warfare as such.

In general, the opinion of the US military is fair if we add the fourth level of information warfare – tool level of application of certain techniques, methods and technologies of information and psychological influence to their three-level classification.

In the Russian information warfare practice, the information operation is understood as a sequence of information attacks divided by periods of exposure, united by an integrated plan and coordinated by time, purposes, tasks, targets and tools of information influence.

3. Research Questions

Each level of information warfare has its own purpose (Table 01). At the strategic level, the purpose of information warfare is not different from the purpose of traditional war: its main purpose is the military

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

defeat of an opponent. It is achieved either by its destruction or by submission of its will (capitulation). In case the information warfare organizer faces a task to maintain the potential and resources of the opponent thus breaking his will to resistance and, thereby, subordinating him, the purpose of information warfare is to ensure voluntary subordination of the opponent expressed by his absolute readiness to follow the will of the curator. For the first time such purpose statement of IW ("ensuring voluntary subordination") appeared in the 1990s in the works of Grachev and Melnik (1999), which remain relevant until now.

At the operational level, the purpose of information warfare is the introduction of attitudes to follow a certain behavioral pattern beneficial for information operation organizers into consciousness and subconsciousness of a person. Thereby the basic principle of voluntary subordination expressed by the readiness of a personality that became an object of information warfare is to follow the behavioral pattern embedded into its consciousness, which is performed voluntarily without any obvious coercion.

There is a variety of behavioral models embedded by information operations organizers into the consciousness of an object. The best known include the model of protest behavior used to disrupt the position of authorities in power and the model of loyal behavior used to support authorities and their political policies. At the same time, external forms of both models can be similar: both representatives of protest electorate and loyalists attend meetings, pickets, demonstrations and other types of mass actions, and, in general, behave similarly. However, some have pro while the other have contra slogans, and the loyalists only attend lawful and coordinated meetings (they support authorities in power).

At the tactical level, the purpose of information warfare is expressed by the introduction of certain patterns for immediate response, mainly in response to an impulse from any external stimulus, into consciousness and subconsciousness of a person. In response to any news opportunity such action may include the desire to go to a meeting, to take part in a demonstration, a procession, the Dissenters' March to support the political initiative, or to join the Maidan.

At the tool level, the purpose of information warfare is expressed by receiving immediate reflexive response to external information stimulus (by the "stimulus-reaction" principle): for example, to stand up for people involved in a fight (having heard "Hey, Rube!") or to immediately go outside thus joining the flow of dissatisfied and angry citizens ready to turn into a political crowd. At the same time, the patterns of strict unconscious actions are embedded into subconsciousness of a person, which he shall make before his consciousness joins the process and begins evaluating the actions of a personality from the rational perspective.

In the USA, the technologies of consciousness and behavior control of people based on external stimuli causing immediate reflexive reaction of an object of information influence are studied within the reflexive control theory developed by Lefebvre (1992) in the 1960s of the 20th century.

Table 01. Four-level structure of information warfare

No.	IW level	Organizational form	Purpose	Relation between levels	Number of attacks
1	Strategic	Information warfare (IW)	**Military defeat** of the opponent. May be achieved by either destruction	Information warfare is a sequence of **information**	**four or more** (at least two CW)

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

			or **submission to a will.**	**operations** united by a single idea and coordinated by purposes, tasks, objects, forms and methods of information influence.	
2	Operational	Information operation (IO)	Introduction of certain patterns to **follow a specific model of behavior** beneficial for information operation organizers into the consciousness and subconsiousness of a person.	Information operation is a sequence of **information attacks** united by a single idea and coordinated by purposes, tasks, objects, forms and methods of information influence.	at least **two**
3	Tactical	Information attack (IA)	Introduction of certain patterns for **immediate response** in response to an impulse from any external stimulus into consciousness and subconsciousness of a person.	Information attack is an operational combination of **certain techniques, methods and tools** of information influence united by a single idea and coordinated by purposes, tasks, objects, forms and methods of information influence.	always **one**
4	Tool	Certain techniques, methods and tools of informational and psychological influence	**Receiving immediate response** to external information stimulus (by the "stimulus-reaction" principle).	-	-

4. Purpose of the Study

The purpose of the study is to define modern information warfare technologies within international relations and world politics, their forms, methods and tools, as well as features of planning and organizational schemes.

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. Research Methods

The study is based on the methods of system analysis allowing identifying and revealing organizational and technological schemes forming the basis of modern information warfare operations; induction, deduction and overt observation.

6. Findings

The standard Anglo-Saxon information warfare represents the sequence of information attacks divided by exposition periods (information silence) and coordinated by time, purposes, tasks and targets.

Using attacks containing deliberately provocative information, the subject to an information attack tries to trigger emotions and inconsiderate acts, which then become a subject of sharp criticism and finally lead to discredit.

Definition: The information attack is the block of specially prepared information stimulating an object of information influence for immediate response (as a response to received external stimulus).

Comment: it is wrong to consider that the information attack shall only contain the compromising information. The information attack may include any stimulating information able to destabilize an object and induce it for immediate spontaneous, unconscious, and adventurous actions. If coarse flattery influences the psychoemotional state of an attack object stronger than a compromising evidence or blackmail, forcing him “to lose the head” (temporarily lose one’s control) under flow of emotions, then the attack will be filled with such information.

Any information warfare operation begins with the information attack towards the attack object (target) or its immediate environment. If one attack is not enough to break the opponent or to subordinate his will, the IW operations use a series of information attacks in public information space consistently through earlier planned time intervals ensuring the effect of exposure.

Definition: The exposure period is the period of information silence dividing two consecutive attacks aimed at reading and analysis of reaction of an object (target) of influence to stimulating information (via positive feedback within the scheme of IW operation). The exposure periods in the scheme of IW operation cover technical pauses; their presence is obligatory.

The scheme of information warfare operation represents repeated (cyclic) process, during which an object is exposed to direct information attack (in the form of information attack provoking an object to immediate action). Its response (with all specific features characteristic of this person) is read through feedback channels is analyzed and gets into the correction mechanism. Based on revealed specific features of an object’s reaction to external information stimuli, its “pressure points”, topics and reasons upsetting the balance of a person are able to immediately excite and bring to extremely unstable “boundary” psycho-emotional state when a person loses the ability to control himself and his actions.

Taking into account the revealed “pressure points” the content of initial information attack is adjusted so that the information influence is focused on problems perceived by the object in the most painful way. Then this attack is again included into the public information space through reference (for the object to an attack) communication channels, and again affects the mentality of an object thus breaking its will to resistance. However, now it is more painful. This continues until the object of an attack completely

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

compromises himself with responses or until his will is completely broken or subordinated to a source of external influence up to complete "suffocation" of the opponent's will by "tightening the anaconda loop around his neck".

To ensure the reliability of information within modern information warfare operations the so-called "operations on legalization of attack information" are used. By nature and functions these are the coverup operations (as they are called by intelligence agencies), which make the attack information reliable, explain its origin (where it was stored, how it got to its present owners) and answer the question on its source of origin – competent or doubtful.

In modern information warfare operations the attacks of compromising information never get into information space unattended – only within the coverup operation (operation on legalization of attack information) performed along with an attack. The operation on legalization of attack information always accompanies the information attack.

The modern information warfare operations utilize three main types of operations on legalization of attack information:

- operations of "controlled leak" of the classified information;
- public statements made on behalf of officials that did not want to be identified;
- public statements of authorized officials (presidents, prime ministers, heads of national intelligence, etc.).

Among the above operations on legalization of attack information the "controlled leak" operations are the most widespread type of coverup operations. The term "controlled leak" came to information warfare from intelligence.

Definition: "Controlled leak" is a special intelligence operation, which purpose is the misinformation of the opponent by transferring him deliberately false or specially fabricated confidential information as authentic and creating the illusion of accidental loss of these data by individuals with access to state secrets due to negligence or carelessness.

Examples: 1) The story on how Hillary Clinton left a folder with documents in a hotel; 2) The Panama papers; 3) CIA monitors journalists (scandal).

In such intelligence operations the classified information is deliberately lost by individuals with access to state secrets (forgotten in hotel rooms, lost on the way, etc.) or is left unattended for some time and at this moment becomes the property of the third parties (letter of credit journalists on a secret site, established intelligence agents of the opponent, etc.) who then make it public having organized an attack in the information space. Rarely the confidential false claims are spread among employees of intelligence agencies that already committed an act of treachery or that is going to become a deserter (for example, Edward Snowden) and then let such person leave abroad having slightly frightened him off.

Statements on behalf of pseudo-officials (anonymous authors claiming to be high-ranking officials of the U.S. Department of State or CIA speaking on condition of anonimity) are also widely used for legalization of information attacks.

The scheme of this operation is very simple: journalists of one of the top-rated TV channels (for instance, CNN or Sky News) release a plot on resonant investigations and exposure where they issue legal proceedings against the object of information attack referring to secret information conveyed by unknown

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

senior staff of the U.S. Department of State or Intelligence Community speaking on condition of anonimity (due to quite known reasons).

Externally everything looks logical and credible in these operations:

- journalists publish data received from their informed sources and they have every right not to disclose their personal data (especially when they deal with the transfer of secret information that the intelligence agencies are chasing for by these sources to journalists);
- nobody will challenge the competence and awareness of the senior staff of the U.S. Department of State or the Intelligence Agency, and usually the public agree with such information by default;
- unwillingness of confidential sources to disclose themselves is also clear and reasonable as their disclosure may lead to immediate arrest on treason charges: having transferred the secret information protected by the state to journalists they have at least committed a serious official crime. Besides, if an intelligence operative acts as a confidential source, then his public statement will inevitably lead to the "exposure" of both himself and his agents, and hence this person shall be removed from operational work and his agency shall be saved at every possible way.

At the same time, in case for some reason a viewer does not believe the legend and will want to be personally convinced of the truthfulness of information conveyed by a TV channel wishing to see the sources himself (to be convinced at least that they really exist and are not invented by journalists), then he will be very disappointed: it turns out that it is impossible to see the persons, which the journalists rely on – the access to them is forbidden. In fact, we are convinced that these persons really exist and bear exposing evidence; however, there is not the faintest chance to check the fact of their existence. It is clear in this situation that journalists act on behalf of anonymous authors who, perhaps, do not exist at all, and actually nobody stole the information from the public space on their behalf: it was prepared by operatives interested in the "controlled leak".

Examples: 1) The Litvinenko's Case – statements made by journalists of the British Sky News on behalf of senior staff of the U.S. intelligence agency speaking on condition of anonimity.

In some cases, the official statements of authorized officials are used to legalize the information (U.S. Presidents Donald Trump, Barack Obama, the Secretary of State John Kerry, the official representative of the U.S. President Administration John Kirby and other authorities).

The principle of this operation is quite simple: a president of a country or his deputy claim that the information in the public space is truthful, reliable and received from a competent source. At the same time, they guarantee by their power, authority and reputation the reliability of data and appeal to trust their word. Many trust them immediately considering that:

- such high officials in enormous authority and enormous trust of voters simply cannot publicly tell lies;
- a president knows what really happens in the country and in the world.

Examples: 1) B. Obama's statement that Russia, Ebola and ISIS are one and the same thing; 2) J. Kerry's statement that Bashar al-Assad cooperates with Islamic State; 3) T. Mai's statement on the case of poisoning of S. Skripal.

Making public statements on the truthfulness of either attack from their official position such figures as the president or the U.S. Secretary of State look extremely convincing; their weight is transferred to

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

information that they truthfully defend. Meanwhile, their high position does not guarantee faultlessness at all: even the presidents of such great power as the USA may consciously use forgery thus deceiving people. There are many examples of such kind: the president Bill Clinton and the Secretary of State Hillary Clinton lied to the U. S. Congress under oath; the Secretary of State Colin Powell consciously misled the UN Security Council having presented a test tube with standard white powder (flour or detergent) for chemical weapons; etc.

In this regard, when making a public statement on September 24 at the UN General Assembly the U.S. President B. Obama said that Russia, the Ebola virus and ISIS represent equal threats to a "free world", and the Secretary of State J. Kerry made a statement that Bashar al-Assad and ISIS are allies, many immediately believed the statements of such senior politicians without getting into content and details, without critical thinking and without challenging the statements of senior government officials on elementary compliance to common sense.

Types of "controlled leak" operations.

In turn, the operations of "controlled leak" of information are divided into four types:

- leak operation performed by provoking journalists to steal confidential materials having no tamper resistance and for a while such materials become available to potential thieves;
- WikiLeaks technologies providing masking of deliberately false (fabricated) data in a big flow of original but invaluable documents;
- "deserter" operations (a typical example of such operation is E. Snowden's escape and story of his prosecution);
- operations of legalization of attacks via public debate ("Psaki-Matthew Lee" technology).

7. Conclusion

1. Multicascade iterative scheme with correction allowing repeatedly applying the method of attacks in relation to one and the same object thus gradually (with each new iterative cycle) bringing him to the required psychoemotional state leading to certain reactions to external stimuli are used in modern operations of information warfare for more delicate attitude to psychological features of an object (target) of influence. The IW operations are based on the principle of repeated (cyclic) repetition of tactical sequence of actions "information attack – technical pause (exposure period)" with obligatory correction of the initial scheme of attack information (alongside with attack content) after each run of the initial iterative scheme (after each iteration).

2. Most often the top officials of the state – a president and a prime minister are subjected to information attacks: as a rule, the information warfare starts with them. The reason is quite simple: top officials are always in crosshairs, they are public people, their every step, each action or movement is considered through a lens. What people forgive to any public politician, even the most senior and known, they never forgive to leaders of the state: they often simply have zero room for error, which to a certain extent makes them similar to sappers. Due to their publicity the top public officials act as chief newsmakers and make the majority of resonant newsbreaks interpreted afterwards by national and foreign media. The information warfare is always centered around top officials, their actions, reactions to either events, which at an initial stage are carefully probed and tested via deliberately provocative attacks of false information,

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

launch of virus content in social networks, distribution of rumors and gossips that emotionally touch at least one of the top public officials and cause his sharp and emotional reaction.

However, a group target may also act as an object of information attack: for example, the political elite of the president – that "inner circle" of authorized representatives, whom the leader of the country relies on. In this case the purpose of an attack is to cause a split into ranks of elite, strive to force them to forget about the interests of the state and to shift completely to save their personal assets. As a result, the leader of the country may be left without support and lose at midpoint.

An information attack may be both directly and indirectly aimed at the president's circle using the "reflected" effect. In his fight against the information attack the leader of the country quite often becomes a transmitter of information influence: by protecting himself, he reflects the information wave on his environment thus repeatedly enhancing its striking effect with his comments.

3. Any operation on legalization of attack information has its markers indicating the use of standard and recurrent legendized techniques of information attacks. All of them fit within the following simple legendization scheme:

a. CIA, State Department, Presidential Administration (department or organization possessing the highest level of competence, ideally being the storage of state secrets) always act as the sources of origin of attack information.

b. Mechanism of penetration of information into public space: theft (always the same).

c. Who stole the information? – an employee of the Intelligence Agency, State Department, special-service agents whose names cannot be disclosed.

d. Natural person through whom the information was legalized in the public space: romantic idealist, justice fighter (J. Assange, E. Snowden, freelance journalists are real people).

e. Why they do not publish all materials at once but give them in pieces? Answer: large volume, takes a lot of time to analyze – "we cannot physically give all compromising evidence into the public space".

The above attributes immediately justify traces of operations on legendization and legalization of attack information in the information noise.

References

DTIC (2005). Joint Publication 3-61 *Public Affairs*. The Defence Technical Information Center. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_61.htm

DTIC (2006). Joint Publication 3-13.3 *Operation Security*. The Defence Technical Information Center. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_13_3.pdf

DTIC (2007). Joint Publication 3-13 *Information Operations*. Retrieved from: http://www.dtic.mil/doctrine/ new_pubs/jp3_13.pdf

DTIC (2010). Joint Publication 3-13.2 *Psychological Operations*. The Defence Technical Information Center. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_13_2.htm

DTIC (2011). Joint Publication 3-13.1 *Military Information Support Operations*. The Defence Technical Information Center. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_13_1.htm

DTIC (2013). Joint Publication 3-12(R) *Cyberspace Operations Defense*. The Defence Technical Information Center. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

FAS (1988). Field Manual 33-1 *Psychological Operations.* Retrieved from: http://fas.org/irp/doddir/army/fm33-1.pdf

https://doi.org/10.15405/epsbs.2019.12.04.286
Corresponding Author: Andrei Manoilo
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

FAS (2014). Field, Manual 3-57 *Civil Affairs Operations.* Retrieved from: http://fas.org/irp/doddir/army/fm3-05-40.pdf

Grachev G. V., & Melnik, I. K. (1999). *Manipulation of personality: organization, ways and technologies of information and psychological influence*. Moscow: Institute of Philosophy, RAS.

Lefebvre, V. A. (1992). *Research on Bipolarity and Reflexivity.* New York: The Edwin Mellen Press.