

## Список використаних джерел

1. Барлетт Дж. FashionEast: призрак, бродивший по Восточной Европе / Джурджа Барлетт; пер. с англ. Е. Кардаш. – М.: Новое литературное обозрение, 2011. – 360 с.
2. Легенький Ю. Г. Философия моды XX столетия / Юрий Григорьевич Легенький. – К.: КНУКІМ, 2003. – 300 с.
3. Маркин Ю. П. Искусство тоталитарных режимов в Европе 1930–х годов. Истоки, стиль, практика художественного синтеза / Ю. П. Маркин // Художественные модели мироздания. Книга вторая. XX век. Взаимодействие искусств в поисках нового образа мира. – М.: Наука, 1999. – С.121–139.
4. Стриженова Т. Из истории советского костюма / Т. Стриженова. – М.: Сов. художник, 1972. – 112 с.
5. Шандренко О. М. Виртуальні образи моди: автореф. дис. ... канд. мистецтвознавства: спец. 26.00.01 «Теорія та історія культури» / О. М. Шандренко. – К., 2008. – 19 с.
6. Шпеер А. Третий рейх изнутри. Воспоминания рейхзминистра военной промышленности / Альберт Шпеер; пер. с нем. С. В. Лисогорского. – М.: ЗАО Центрполиграф, 2005. – 654 с.

## References

1. Bartlett Dzh. FashionEast: prizrak, brodivshiy po Vostochnoy Evrope / Dzhurdzha Bartlett; per. s angl. E. Kardash. – M.: Novoe literaturnoe obozrenie, 2011. – 360 s.
2. Legenkiy Yu. G. Filosofiya modi XX stoletiya / Yuriy Grigorevich Legenkiy. – K.: KNUKIM, 2003. – 300 s.
3. Markin Yu. P. Iskusstvo totalitarnykh rezhimov v Evrope 1930–h godov. Istoki, stil, praktika hudozhestvennogo sinteza / Yu. P. Markin // Hudozhestvennyye modeli mirozdaniya. Kniga vtoraya. XX vek. Vzaimodeystviye iskusstv v poiskah novogo obraza mira. – M.: Nauka, 1999. – S.121–139.
4. Strizhenova T. Iz istorii sovetskogo kostyuma / T. Strizhenova. – M.: Sov. hudozhnik, 1972. – 112 s.
5. Shandrenko O. M. Virtualni obrazi modi: avtoref. dis. ... kand. mistetstvoznavstva: spets. 26.00.01 «Teoriya ta istoriya kulturi» / O. M. Shandrenko. – K., 2008. – 19 s.
6. Shpeer A. Tretiy reykh iznutri. Vospominaniya reykhministra voennoy promyshlennosti / Albert Shpeer; per. s nem. S. V. Lisogorskogo. – M.: ZAO Tsentrpoligraf, 2005. – 654 s.

**Капитоненко О. М.**, research, National Pedagogical Dragomanov University, (Ukraine, Kyiv), a321831@gmail.com

## Fashion totalitarianism and post-totalitarianism as a sociocultural phenomenon

*The problem of totalitarianism culture is still poorly understood. In the Soviet Union the socialist fashion starts forming since 1930s, dominating in Eastern Europe since the mid 1950s. Moscow Fashion House managed fashion trends and was in fact one of the major components of the Stalinist cultural myth, which defined the image of fashion product as «ideal clothes». Formed this way, the socialist good taste with its criteria of modesty and conservatism was firmly rooted in the daily life as officially recognized aesthetic canon.*

**Keywords:** fashion, totalitarianism, political advance-guard.

**Капитоненко А. М.**, соискатель, Национальный педагогический университет им. М. П. Драгоманова (Украина, Киев), a321831@gmail.com

## Мода тоталитаризма и посттоталитаризма как социокультурный феномен

*Проблема культуры тоталитаризма еще мало изучена. Прежде всего, теоретики описывают общие тенденции, какие происходили в искусстве, – это нивелирование, образные упрощения и определенная подчиненность всех процессов, которые происходили в культуре, их зависимость от политики. Можно утверждать, что режимы Гитлера, Муссолини, Сталина были эквивалентными с точки зрения осуществления тотального контроля над культурными реалиями в обществе. С 1930-х годов в Советском Союзе уже начинает формироваться социалистическая мода, а с середины 1950-х годов доминирует в Восточной Европе. Московский Дом моделей был фактически одной из главных составляющих сталинского культурного мифа, в котором образ модного изделия все больше и больше становится образом, который можно отметить как «идеальная одежда». А появление сети региональных Домов моделей завершило строительство советской иерархической системы управления. Сформированный таким образом, социалистический хороший вкус, с критериями скромности и консерватизма, прочно вошел в повседневную жизнь, как официально признанный эстетический канон.*

**Ключевые слова:** мода, тоталитаризм, политический авангард, мегаломания.

\* \* \*

УДК 101.1:316

**Hajiyeva R. A.**,  
PhD student, Institute of Philosophy and Law National  
Academy of Science of Azerbaijan (Azerbaijan, Baku),  
matlabm@yandex.com

## INFORMATION WAR

*Article is devoted to information warfare various environmental forces in the modern period. The article analyzes the characteristics of these wars, the recommended way of protection from information hostile invasion.*

**Keywords:** information war, ideology, exposure.

*(стаття друкується мовою оригіналу)*

This is an American concept that tries to explain the information management technology in order to gain a competitive advantage over the major rivals in the ammunition industry. The information war is a protracted war that commenced long before the world wars but became real immediately after the Second World War with the rise of the cold war—ideology war between USSR and the United States of America. The information warfare is a warfare that involves gathering of tactical information that may be full of propaganda but in the context of reality, they may be deemed valid [1].

The information war is directly linked to the psychological warfare because it is actually a warfare that is aimed at demoralizing the intentions of the major opponents. The America's main focus on the information warfare is based deeply on its level of advanced technology and expertise and therefore, the American nation has an ill motive to extend its' scope into the field of the warfare of electronics, cyber war, computer network operations attack and defense and the information assurance warfare. However, the kind of war also adopts the human related perspectives of the use of information; for example, the information warfare takes into account the use of human command and control, social network analysis as well as the analysis of decisions.

## Types of Information War

There are so many kinds of the information warfare that has been noted and well defined since the inception of technology. This information warfare types are very offensive and defensive given the fact that it has very detrimental effects on others while the main contenders have one major slogan of protecting their own interests and ill motives. The actions that are formulated under the brink of the kinds of warfare are designed to achieve advantages over military or business adversaries [2, p. 311–313].

There are seven major types of information warfare that have a common goal of denial access of any necessary and important information, degradation, protection and most importantly manipulation and propaganda. The major seven types include: the hacker and cracker warfare in which computers are directly or indirectly attacked by different kinds of viruses, the cyber warfare that involves very unfortunate scenarios of grabbing bags, the economic information warfare that involves providing a barrier to business information flows and channels hence aimed at pursuing economic dominance, the command-and-control warfare which is the most fatal and dangerous because it involves striking at the foes' head or neck. This sounds like a real warfare but the fact puts it very straight that it is not a real warfare [3, p. 42].

The other types of information warfare include the psychological war. In this kind of warfare, the information that is gathered from various sources are used to change the

minds of enemies, the neutrals as well as the friends with an ill motive of dominating the world economically and in accordance with the military strength and the power base—arms race [3, p. 57]. The intelligence-based warfare involves the design, denial access of systems and protections that is aimed at gaining sufficient knowledge, skills and expertise that can be adopted to conquer the battle space. Lastly, the electronic kind of warfare that uses cryptographic techniques to spread propaganda against the enemy so that the enemy can get dissuaded from achieving its objectives because it is denied access to systems and important information that can help spur development.

The old forms of propaganda and control are not vanishing but they are being supplemented with new emerging forms that have been deemed fit to reach so many people across all corners of the world. The information warfare has not diverted the adoption of the real warfare tactics because at the present times, several governments of the day are trying to increase the budget in order to accommodate the demands of the rising security forces that are in control of the major streets and at the same time, they have devoted their interests and efforts to have control of the information highways [4, p. 845].

The cyber warfare is a politically motivated in attaching and hacking computers or electronic gadgets in order to conduct sabotage and espionage. It is a kind of information warfare that is seen as a backward warfare—a warfare that is provoked by cheap politics of the day. The United States of America's security experts have defined the cyber warfare as actions that one country formulate to invade other country's computers and networks in order to cause disruptions and mayhems that will automatically destabilize the government. The American nation has declared that the America's digital infrastructure is a national asset and therefore they have put forth several interventions to defend the military networks and at the same time attack other superior nations networks in order to cause damages and disruptions of the governments of the day hence weakening their economic and military power [5, p. 278].

The hacker warfare technique normally adopts the Denial-of-service (DoS) attack whereby an attempt is made to make a resource unavailable for the major uses. This is done through crushing the several computer components so that the machines cannot operate at all or the machine is denied access to network hence the internet which is a major source of information become useless to the users. However, it is of interest to note that the perpetrators of DoS attacks normally targets very crucial services that are supported by the major web servers e.g. the banks, credit card payment gateways such as the automated teller machines etc. these services forms the heartbeat of the economic development of a nation and therefore if they are affected, the economic development of the state will be completely paralyzed and disrupted hence weakening its economy. This will cause a lot of devastating effects and it will automatically destabilize the government of the day [3, p. 63].

The information warfare types are commonly used to conduct sabotage. Computers and satellite are major information components that are targeted in order to cause disruptions because they coordinate major government activities across the whole world. The General Keith B. in America recently informed the senate armed service committee of the United States that the computer network warfare is at the climax of its emergence and it has caused a

lot of disparity between the America's capability and power to perform some operations and the rules and regulations that governs the conduct of both the national government and the state governments [6, p. 129–150].

The information warfare types have been so common in the modern times to the extent that the distributed internet based attacks gives an implication that it is very difficult to catch the motivating and the attacking parties. This tries to elucidate that it has become very much challenging to make a conclusion to whether the attack is an act of war or not. There are various examples of the information warfare types across the whole globe that has been attributed to political motivations and hysteria. In the year 2008, the former Union of Soviet Socialist Republics now Russia commenced a cyber attack to Georgian government website. This was conducted in conjunction with the military operations that took place in South Ossetia. During the same year, the Chinese government also came out to defend their protracted attempts to instigate the information warfare. The Chinese nationalist hackers attacked CNN to seek revenge given the fact that CNN came out clear and announced on Chinese repression on Tibet [7, p. 199–222].

### **Purpose of Information Warfare**

The purpose of the information warfare is four-fold. The main intention of the kind of war on the cyber attacks is aimed at affecting and destabilizing the existing economies of several competing states. The economies destruction is the main intent of the information warfare because it gives support to four very important infrastructures: the power grid, transportation, financial as well as communication infrastructure. These are the four major things that act as the building blocks of superior economies and dominance.

The kinds of the information warfare are a good option for the United States of America to advance its interests in foreign policies. The nation of America possesses great technological knowledge and experiences and this is the major factor that is prompting the nation to wage the information war against other states which are competing with the nation. Most of the cyber attacks that the United States of America hoisted occurred at around 1994. During this time, the administrators of the computer systems that are situated at Rome Air development Center went overboard to discover a sniffer program that was installed on one of the systems that they owned then. The sniffer was strategically installed at the center because the laboratory of Rome is one of four Air Force super laboratories and a national center that develops new technologies for command, control, communications, computers and intelligence [3, p. 69].

This therefore implies that installing a program to hack the systems of this laboratory would cause serious damages and disruptions that would have caused total destabilization of the government. The installed program was used to gather and access information from other military, governments, commercial institutions and even foreign militaries hence giving a clue on major interventions that they could electronically employ to cause serious damages and disruptions to other emerging states [5, p. 271–282].

The American government has also employed the information warfare in order to exploit the insecurities of the networked globe. Through the information warfare the United States of America's intelligence has gain access to the European parliament and the European Commission with an ill motive of a global espionage campaign. The major intention

of the espionage campaign is to steal secrets of both political and economic nature of other superior European nations like Britain, France, Russia, China, Italy etc. Given the fact that the European parliament computer component systems were manufactured by the American firms; the American nation has taken an advantage of this and therefore they have used internet routers in order to access the internal network of the parliament hence retrieving very confidential information that can help them to intervene several strategies to bring down the economies of other states and maintains the world dominance in terms of its economic power [8, p. 41].

The officials of the European parliament and commission have also put forth claims that the United States of America has used its massive technology power and prowess to conduct an electronic raid that helped them to destabilize the General Agreement on Tariffs and Trade (GATT) last year. This puts the matter very straight that the American nation is determined to use its technological advancement expertise to exploit the world by causing disharmony and crushing the components of major world organizations computer systems that is aimed at paralyzing their operations hence helping to create mistrust that ultimately causes failure. It is logical to note that the American state is a very jealous state, a state that does not want to see other states prosper because they have a feeling that the emerging nations may out-compete them if they fail to act against their operations.

#### Methods

It is undisputed truth that the United States of America has one of the most developed electronic infrastructures in the world. The American state has majorly adapted to methods to wage the information war against other nations. The methods include: offensive information warfare and defensive information warfare. However, the information warfare is more concentrated on defensive actions rather than offensive actions. The offensive warfare method involves employing various actions in an attempt to thwart the development of other nations because of the fear of competition. The United States has been at the top most position since the end of the Second World War which marked the beginning of the cold war.

It has maintained its position as the world superpower for two major reasons; one, because it possesses enormous resources and two, it exploits other nations. The information warfare is just one way that the American state devised to thwart any possible attempt that any other nation may have to rise to the same position that the nation is proud of. The defensive information warfare method is a method that the American state has employed to defend and protect their superiority in the field of technology as well as the world economies. The DoD and the IC have done a commendable job in identifying and adjusting to the new national security threat posed by information warfare. However, there is still work to be done. The American nation should be guided by ethical principles to shun the war [1, p. 9].

In a broader sense, information warfare is a war that involves the process of communication. The gamble for power commenced with the emergence of human communications and conflict. However, the American state should take a sole responsibility of the devastating effects of this kind of war because it is a war that was devised by the American intelligence [5, p. 271–282]. It should be noted that the information warfare has led to increased rate of online terrorism and it has also sparked real war in some parts of the

world. In order for the warfare to end, the United States of America must be at the forefront to conduct campaigns and build effective firewalls that can guard the attack of computer systems by the use of its advanced knowledge in technology. The information war begun in America and so it must just end in America but the government intervention. The American nation should be guided by the ethical principles and the rule of morality to bring the information warfare to an end because what the nation is doing strongly compromises the ethical standards and the rule of morality.

#### References

1. Grant Osborne et al., «Dynamic Content on Support of the User-defined Operational Picture». Journal of Battlefield Technology 12, no. 1 (2009).
2. Rakhmonov Ulugbek, «Information Terrorism—a New Kind of Terror in the Global Information Arena». International Journal of Business & Social Science 3 (2012).
3. Edward Waltz, Information warfare: principles and operations / Edward House, 1998).
4. Jonathan Reed Winkler, «Information Warfare in World War I». Journal of Military History 73, no. 3 (2009).
5. Neil Metcalfe, «A short history of biological warfare». Medicine, Conflict and Survival 18 (2012).
6. Paul Bolt and Carl Brenner, «Information Warfare across the Taiwan Strait». Journal of Contemporary China 13 (2004).
7. Iain Munro, «Defending the Network Organization: An Analysis of Information Warfare with Reference to Heidegger». Organization 17 (2010).
8. Joint Chiefs of Staff, Information warfare: legal, regulatory, policy and organizational considerations for assurance / prepared by Science Applications International Corporation, Telecommunications and Networking Systems Operation (Washington, DC: Joint Chiefs of Staff, National Defense University, 1995).

*Гаджиева Р. А., докторант, Інститут філософії та права Національної академії наук Азербайджану (Азербайджан, Баку), matlabm@yandex.com*

#### Информационные войны

*Статья посвящена вопросам информационной войны разными идеологическими силами в современный период. Анализируются характеристика этих войн, рекомендуются шляхи захисту від ворожої інформаційної навали.*

*Ключевые слова:* информация, война, идеология, вплив.

*Гаджиева Р. А., докторант, Інститут философии и права Национальной академии наук Азербайджана (Азербайджан, Баку), matlabm@yandex.com*

#### Информационные войны

*Статья посвящена вопросам информационной войны различными идеологическими силами в современный период. Анализируется характеристика этих войн, рекомендуются пути защиты от враждебного информационного нашествия.*

*Ключевые слова:* информация, война, идеология, воздействие.

\* \* \*

УДК 101.8

**Ігнатко В. С.,**  
здобувач, Національний педагогічний університет  
ім. М. П. Драгоманова (Україна, Київ),  
gileya.org.ua@gmail.com

#### БЕЗМЕЖНІСТЬ «ЖИТТЄВОГО ПРОСТОРУ» ЛЮДИНИ ЕПОХИ ІНФОРМАЦІЙНОЇ РЕВОЛЮЦІЇ

*Аналізується зміна характеристик життєвого простору людини в процесі становлення інформаційного суспільства; головним індикатором цього процесу є інтелект, який не тільки змінює вигляд життєвого простору, але й встановлює його нові контури; останнє визначається поняттям «безмежність»; автор стверджує, що досягнення зазначеної мети в масштабах людства є можливим на засадах фундаментальної зміни парадигми суспільного мислення – від домінуючого нині споживацького утилітаризму до формування мислення нового типу – ноосферного, яке передбачає можливість і здатність людей*