ISSN:0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 5(F), pp. 26859-26866, May, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

ResearchArticle

INFORMATION WARFARE CONCEPTUAL FRAMEWORK

Monov, LB[1]*and Karev ML[2]

[1]Directorate "Strategic planning", Ministry of Defence, Sofia, Bulgaria
[2]Defense Advanced Research Institute, G. S. Rakovski National Defense College, Sofia, Bulgaria

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2139

ARTICLE INFO

Article History:
Received 10th February, 2018
Received in revised form 6th March, 2018
Accepted 24th April, 2018
Published online 28th May, 2018

Key Words:

Information warfare, social media campaign, cyber operations, strategy, influence operations.

ABSTRACT

We investigated the concept of information warfare with an aim to provide a contemporary theoretical framework for its understanding. We think that information warfare is a strategy that uses multiple venues in a synchronized way to destabilize societies and to manipulate the bound between populations and governments. We concluded that its conceptual framework encompasses four branches of operations in: electromagnetic spectrum, traditional media, social media and cyber space. It includes a system of below and above the line of peace and war activities that have to destabilize societies and to manipulate governments. The goal is to spread influence and to control circumstances which represents a form of trans-border security threat. This situation of strategic disturbance is a form of limited war, a concept of dominant power, which depends upon degradation in freedom of actions, erosion of trust in institutions, ideas and values; disruption in decision-making process and discord in society.

INTRODUCTION

The subject of information warfare has been around since the beginning of the1990s. The prime reason for this was the giant jump in the area of communication technologies and Internet that brought strategic consequences for governments, armed forces and population. In fact, the global democratization of information has provided a wide-open window for business opportunities and personal development while it has allowed a progressive erosion in the area of national security. The free and unrestricted flow of information has managed to reach places that have never been reachable before. First and foremost, this is the human mind as a central fabric of social life and main carrier of values. Indeed, the uncontrolled use of cyberspace for communications has provided a bridge for fake news, propaganda and messages of violent hatred that have influenced human behavior. Second, global dependence of information networks has set some new prospects for deep penetration into political establishment including unlimited interference and control over decisions and actions. Governments, private companies and Internet moguls have managed to exploit people's diverse interests that changed their mindset. To some extent, the information revolution puts national governments at a critical juncture between responsibility to protect their sovereignty and lawful functions without obstructing the constitutional rights of their citizens. That is why David Rothkopf argues that national security establishment has to solve some of the most difficult issues about cyber war, privacy and surveillance, about taxation and who controls the Internet (Rothkopf, 2014).Certainly, the information has a huge potential to cause chaos, to divide people, to alter politics and to paralyze decisions and actions. In this context, working with information someone may set a number of opportunities to spread influence and to control circumstances that would serve its ultimate goals. At the heart of this statement is the general hypothesis that information warfare is a type of strategy that uses multiple venues in a synchronized way to destabilize societies and to manipulate the bound between populations and governments. Moreover, information warfare is a proactive choice that bypasses traditional defense borders and puts the target in a situation that blurs the line between rational and irrational choices and actions. Consequently, it might be a destructive weapon that slides below the threshold of war.

RESEARCH METHODOLOGY

In this paper, we investigate the concept of information warfare with an aim to provide a contemporary theoretical framework for its understanding. In order to do so, we have conducted a

*Corresponding author: **Monov, LB**
Directorate "Strategic planning", Ministry of Defence, Sofia, Bulgaria

content analysis of several official documents of the USA, NATO, EU, some research papers, books and open-end opinions that discuss the subject. Considering how wide and different are our sources and in order to comprehend their key ideas we focused our attention on these specific categories that identify the general concept of strategic theory. Our central assumption is that on the global arena different actors will use different strategies to compete for power. As Colin Gray insists "*Strategy is adversarial; it functions in both peace and war, and it always seeks a measure of control over enemies (and often over allies and neutrals, too)*." (Gray, 2016)

Investigating information warfare as a strategy for manipulation and destabilization, first we analyzed the US Intelligence Community Assessment - Assessing Russian Activities and Intentions in Recent US Elections and the Special Counsel of the U.S. Department of Justice Indictment against Russian based Internet Research Agency LLC. We were searching for three basic categories that are generic for strategy formulation, namely - objectives, ways and means. Also, we used definitions (table 1) for these categories that helped us to organize the process and to standardize the results. (Yarger, 2006)

Table 1 Strategic Logic Analysis Matrix

Category	Description
Objectives	The desired final outcome, or "what is to be accomplished"
Ways	Courses of actionfor using the available resources
Means	Capabilities and resources that are available or can be developed for implementation

We determined our work on this fabric that connects someone actions to exercise control over the environment with resources to accomplish his objectives. Specifically, we applied concept-mapping technic to identify main ideas form our sources, we grouped them in a new perspective and we generated an information warfare generic map. Furthermore, we have examined some sources with Russian point of view that served as a control of our hypothesis. In other words, after breaking down the subject of information warfare into parts, we unified them in categories; we analyzed them and abstracted the overall conceptual structure of information warfare.

Instead to research the subject from a purely military point of view we looked at it as a national strategic problem. Consequently, here we do not speak about the gist of electronic warfare and psy-ops, which belong to the military instrument of power.

Russia's Information Warfare against the United States of America

The topic of Russia meddling into the US political life is probably one of the most controversial issue that political leadership, media and security experts have discussed lately. Most of them have agreed that it has a potential to undermine the stability of Washington's political process deep to its roots. Also, they claimed that Moscow conducted well-planned and organized information war against the USA. The ultimate object of this approach was to paralyze political process and to corrupt American way of life. (Mckew, 2017)Despite the fact that there are diverse opinions how successful Russian strategy was, it is obvious that it brought up many questions about sovereignty and political stability. Taking advantage of some disruptive U.S. political and social issues as well as undergoing dynamics in social networks Russia used a multiway approach that combined traditional media operations, cyber-attacks and social media operations. Therefore, their joint and synchronized utilization represent information warfare as a strategy for manipulation and destabilization with one goal – to create political instability. Indeed, well planned and conducted interference efforts have enough charge to mislead the public about the state of reality while providing enough options for strategic impact.

The US intelligence community considers that Russia intentionally conducted influence campaign targeting the 2016 US presidential election with goals "*to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency*". (Office of the Director of National Intelligence, 2017) They deliberated that Moscow had settled an approach, which had to advance the election of Donald Trump as a president. This strategy encompassed open state-media efforts of Moscow and covered operations of paid agents. National intelligence described this as a multiphase campaign that additionally included cyber espionage, public disclosure of collected data, cyber intrusions into electoral boards. Furthermore, the analysis implies that Moscow carefully planned and prepared its actions.

Another document, the Indictment against one private company and thirteen Russian citizens, claims that the defendants intentionally conspired "*for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016*". (Department of Justice, 2018) The accusation also displays strategic approach that encompassed reconnaissance, analysis, planning, preparation, actions, command and control including measurement of success. This includes a combination of acts in social networks as spreading political advertisements, staging political rallies, posting derogatory information, supporting radical groups etc. On the cyber side, Russia ran cyber-attacks for identity theft and content stealing including unauthorized access to servers and information. In support of propaganda efforts Moscow used fake personalities to produce content, to write blogs, posts, and comments.

Certainly, we discovered that both documents used term "information warfare" to explain Russian activities, but in fact, they did not define its meaning. Consequently, this triggered our interests so we looked at different sources that discuss the subject of information warfare. After mapping these two documents, we concluded that the Russian approach is an example of strategic influence, which brings together a combination of well-defined proactive tactics with appropriate means. This strategy included at least two distinguished phases and had one ultimate goal to create political instability(table 2). Phase one – Preparation was designated to set appropriate conditions for interference with the US political system. Here from the end side, we see three specific objectives - to inform interference and influence operations; to hide the Russian origin of their activities; and to reach significant numbers of Americans. The ways part included multiple actions ranging from intelligence collection for political parties, leaders, think-thank organizations and lobbyist; procuring and using

computer infrastructure; creating of social media accounts, social media sites and group pages.

Table 2 Basic Map - Russia's information warfare against the United States of America

Phase One – Preparation		
To set conditions for interference with the U.S. political system		
Ends	**Ways**	**Means**
To inform interference and influence operations	- Intelligence collection for political parties, leaders, think-thank organizations and lobbyist - Tracking and studying groups on U.S. social media sites dedicated to U.S. politics and social issues - Traveling to the United State	- Computer infrastructure, based partly in the United States - Individuals, private organizations - Financials resources - Social media platforms- YouTube, Facebook, Instagram, and Twitter - Groups in social media
To hide the Russian origin of their activities	- Purchasing space on computer servers located in the USA - Registering and controlling of web-based e-mail accounts hosted by US providers - Operating with numerous different banks and multiple bank accounts in the USA	
To reach significant numbers of Americans	- Creating of social media accounts - Creating thematic group pages on social media sites - Creating and posing as U.S. grassroots entities and persons - Contacting to U.S. political and social activists - Theft identification - Developing certain fictitious US persons into leaders of public opinion	
Phase Two - Execution		
To manipulate electoral process and destabilize the bound between population and government		
Ends	**Ways**	**Means**
To support and promote the presidential campaign of then-candidate Donald J. Trump	- Producing materials about the presidential election and using electronically related hashtags - Soliciting and paying real U.S. persons to participate or perform certain tasks - Supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements - Staging political rallies inside the United States	- Unwitting individuals - Political activists, volunteers and supporters - Grassroots groups - Social media YouTube, Facebook, Instagram, and Twitter - Financial resources - False identities
To disparage Hillary Clinton	- Buying political advertisements - Posting derogatory information - Encourage U.S. minority groups not to vote in the 2016 U.S. presidential election or to vote for a third-party U.S. presidential candidate - Promoting allegations of voter fraud by the Democratic Party	

Phase Two – Execution had to manipulate electoral process and destabilize the connection between population and government. In order to do so Russia used hackers and social media to support and promote Donald Trump and to disparage Hillary Clinton. The successful accomplishment of these goals required arrangement of activities in cyber domain and social media ecosystem that recognize the power of unwitting individuals, marginalized political activists, volunteers, supporters and grassroots groups to shake the political life. Their actions encompassed everything possible starting from content creation and dissemination, comments on emigrations and border security, political advertisements against Secretary Clinton, posting derogatory information for Democratic Party, attacks on mainstream media, focus on racial and religious differences, staging political rallies in support of Donald Trump and against Hillary Clinton. Finally,all this resulted in two different partisan reports of the House Intelligence Committee, the special prosecutor, multiple reports, numerous Russia-related investigations and subpoenas, millions of tax-payers money, hundreds of TV hours, dissemination of speculations, a rise of conspiracy theories that in fact destabilize the political establishment in Washington.

From a pure theoretical point of view, Russian strategy demonstrated a successful long-distance non-kinetic warfare that bypassed traditional defense borders, economic and military superiority. It showed that combination of traditional media messages, cyber-attacks and social-media campaign might set the ground for influence over population and control of choices. In fact, transmission of narrative on controversial social and political subjects increases the gap among different groups and puts the connection between population and government under pressure. This strategy slides below the threshold of open confrontation including military and may be classified as information warfare.

Information Warfare – A Conceptual Framework

Nowadays information warfare has multiple names, many dimensions and numerous purposes. With modern technologies and sophisticated means of messaging it represents a form of limited war, which carries a low level of escalation while, provides opportunities to advance geopolitical goals at minimum cost. In fact, information warfare is a type of transnational threat to the national security that penetrates national borders and affects stability. It is about the influence over population and leaders as well as control over decisions and actions.

From a military point of view, the term information warfare does not legally exist. However, military instrument of power considers the complex reality of modern battlefield and the importance of information for the operational outcome. The general understanding is that information is a conduit that connects all operational efforts towards one end-state. For example, the last publication of the US Department of Defense Dictionary of Military and Associated Terms defines information operations as '*integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.*" (DOD Dictionary of Military and Associated Terms, 2018) The dictionary also refers as separate activities -electronic warfare; military deception; military information support operations. Another source – NATO Glossary of Terms and Definitions speaks about information activities as "*actions designed to affect information or information systems*."(NATO, 2017)The

Alliance also considers the importance of electromagnetic spectrum for the success of armed forces operations. Consequently, NATO defines electronic warfare as "*military action that exploits select electromagnetic energy to provide situational awareness and achieve offensive and defensive effects*." (NATO, 2017)However, the document does not explicitly outlines the term information warfare. In addition, EU does not accept information warfare as one entity. The organization considers the importance of information activities as an enabler of success and defines information campaign as a set of activities that support the goals of Crisis Information Strategy (EEAS, 2016). Still, EU fully comprehends the danger from propaganda, cyber-attacks and disinformation to the stability of the alliance and its member countries. Therefore, EU considers different approaches and instruments to resist against them. For example, EU has established the East StratCom Task Force which main task is to fight Russia's ongoing disinformation campaigns. The Task Force reports on and analyses disinformation trends, explains and corrects disinformation narratives, and raises awareness of disinformation.

The information warfare does exist in the wide public space. Its current vision is widely stretched between different categories and areas of expertise. Furthermore, numerous scholars and security experts use information warfare to describe complex activities, which a malicious actor applies in cyber space or public relations or electromagnetic spectrum separately or simultaneously to accomplish its goals. These actions vary from propaganda, disinformation, cyber hacks, electronic intelligence, surveillance, jamming, content creation and dissemination. Over time, they have been referred to influence campaign or messaging strategy, social media disruption operations, psy-ops, manipulation campaign or sophisticated war.

As a general strategy, information warfare includes four clearly distinguished types of operations, which we divide into two categories. First, we formulated above the line of peace and war operations that embrace - traditional media operations and electronic warfare. For example, they encompass acts that have a clear source and use traditional approaches to spread messages and to engage with targets in electromagnetic domain. Second, below the line of peace and war operations include cyber-attacks and social-media operations. They comprise actions that rely on modern technologies to cover the source, to steal information, to damage cyber networks and assets and to put right communications in front of the right person at the exact time. (figure 1)Linked and synchronized together towards one goal, above the line and below the line of peace and war operations represent a strategy of dominant power. Doctor Cathy Downes describes a similar situation with two terms namely "*narrative power*" and "*disruptive power*" both linked as an instrument of strategic influence, which consider national developments and "*capabilities of interactive social Internet*". (Downes, 2018)

The question of Information warfare as a tool of influence has been discussed in multiple articles and research papers. One prominent scholar, Sir Lawrence Freedman insists that current state of affairs sets multiple opportunities for states and individuals to disable systems, which work with information, and to influence perceptions of the population.

Mapping information warfare

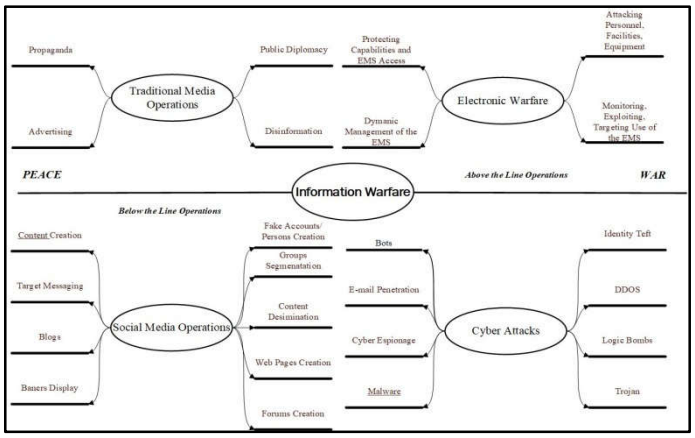

Figure 1 Information warfare general map

Besides, the Internet ability to share ideas and narratives brings the conflict to the social level of society. This approach - information campaign depends on the content and represents part of information war that could create "*false impressions in order to construct or break allegiances and sympathies*." (Freedman, 2017) In other words, it raises strain and friction on current issues between different groups and opinions and brings discord in society. The author asserts that cyber war is the other part, which has a purpose to complicate the environment and irritate population. It utilizes malware like viruses and warms to infect computers and networks to disrupt the functionality of infrastructure and data.

David Stupples considers Information war as a combination of three distinctive type of warfare for attack and defense with a specific purpose. First, it includes electronic warfare that has to disrupt electromagnetic space. Second, it takes in action cyber-attacks to affect the functionality of national infrastructure. Third, it comprises psy-ops, which have to degrade the moral and undermine values and norms. Finally, their joint utilization would cause instability and chaos. (Stupples , 2015)

Some experts argue information warfare changes the cost-benefit analysis by sowing doubt about ethical positions, ideas and principals. Communication on these topics can be done through well-known networks of TV channels, printed outlets and radio stations. For instance, Helle Dale from the Heritage Foundation maintains that trough the state-owned TV Russia Today, Moscow conducted Information warfare to spread propaganda and disinformation in order to undermine the US and Western credibility and to make Russia looks good. (Dale, 2015)Indeed, the channel represents a type of global network that has to manifest Moscow' strength and to present alternative views via broadcasting in Central Asia, Central and Eastern Europe and in the West including the USA.

Information warfare is "shadow war" and "war on truth" that applies political advertisements and target messaging to altered politics, to destabilize relations with friends and allies, and to rift public. The most important purpose of such war is that target acts against its own interests. (Mckew, Forget Comey. The Real Story Is Russia's War on America, 2017)Here boundaries do not exist because the attacker may use state-owned media to spread openly confusion and distraction and to advance its political agenda as well as patriotic hackers or non-state actors to create an artificial environment. It is also a "war

of narrative" that uses social media to manipulate facts, disperse misinformation, and amplify on diverse issues. Additionally, this type of war applies cyber-attacks to hack voting machines and steel private information with final purpose to delegitimize democracy. (Mahaffee, 2018)Consequently, this is a classic example of a strategic approach that has a potential to erode trust and credibility of institutions and to create discord in the society.

In this respect, information warfare follows three avenues. First, the attacker collects information on specific targets and groups in order to understand their differences, preferences, desires and weaknesses. It also considers people's diversity as geographic location, cultural bias, behavioral pattern, political deviations and demographic to widen the gap between communities and to increase the level of uncertainty.

Second, it creates and spreads narrative to the target audiences and individuals trough available media channels. Some pundits argue that it represents a type of refined media offence "*to influence hearts and minds by bypassing traditional media outlets*". The central part of this approach is an exaggeration of some stories and understatement of others. (Torossian , 2016) It exploits biggest fears, internal outage and doubts to cause deliberate damage to the trust in institutions, ideas and values. In order to accomplish its goals governments or organized non-state actors combine different methods such as "*false news, disinformation, or networks of fake accounts aimed at manipulating public opinion*". (Weedon, Nuland, & Stamos, 2017) His goal is to influence the target by distracting from a specific event and redirect it attention to different direction. It may use regular media to deny or reject allegations, to present multiple interpretations of the specific event and to send propaganda and public diplomacy messages. In addition, it could amplify its activities by using a current social-cyber network to micro-target with political advertisements, banners, proposals and false stories. According to the Facebook General Counsel, Colin Stretch during 2016 presidential elections for about two years the network provided the platform for distribution of 3,000 Facebook and Instagram ads that promoted roughly 120 Facebook pages. Additionally, 29 million people posted content form Russia originated operations 80,000 posts that approximately reached 126 million people.(Stretch, 2016)

Finally, it increases the scope of its efforts in order to recruit supporters and solicit resources. Furthermore, trough network of supporters, fake personalities, botnets and trolls the attacker intensifies the level of his activities to create an artificial environment of diverse opinions and to erode the credibility of information. There is information that during the US presidential campaign of 2016 just for one month 400,000 bots were engaged in the political discussion that were responsible for about 3.8 million tweets. According to the researchers, social bots could generate tangible results to polarize the debate, to redistribute influence and to push the agenda forward. (Bessi & Ferrara , 2016)Rebecca Goolsby describes this as a "social cyber-attack" that promotes chaotic mass behavior, escalation of rumor, confusion, panic, and violence. (Goolsby, 2013) In this case, the adversary reaches its final goal to maintain control over the situation.

Information warfare is a dangerous tool that relies on technological vulnerabilities, interdependent communication networks and human desire for information. According to Bill Gertz modern conflict is a form of non-kinetic struggle, a new kind of war - iWar that encompasses "*technical cyberattacks on networks that run everything and content-oriented, sophisticated information war that uses a wide array of information tools as weapons*." (Gertz, 2017) Its decisive aims are to produce discord in society, to disrupt decision-making process and to degrade freedom of action without or with little physical destruction. From a security point of view this can be translated as the destruction of American nation its ideas and values.

The conceptual theoretical framework of information warfare

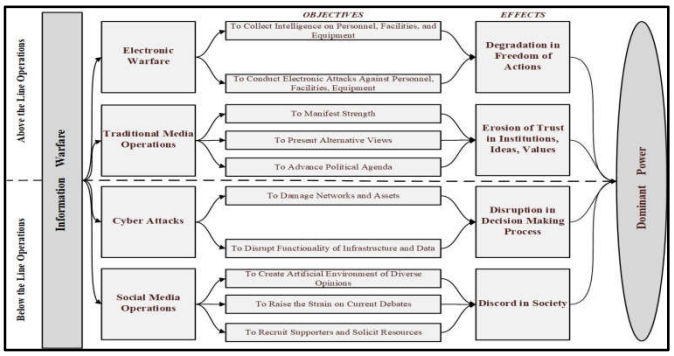

Figure 2 Structure of Information Warfare

In short, the conceptual theoretical framework of information warfare (figure 2) encompasses four distinctive branches of operations with specific objectives and desired effects. It includes a system of below the line and above the line of peace and war activities that have potential to destabilize societies and to manipulate governments. The final goal is to spread influence and to control circumstances. Linked and synchronized together they build a cumulative effect that represents a form of trans-border national security threat. Indeed, this situation of strategic disturbance represents a form of limited war, a concept of dominant power, which depends upon degradation in freedom of actions, erosion of trust in institutions, ideas and values; disruption in decision-making process and discord in society.

Russia's Point

In Russia there are different opinions about information warfare applicability in the area of strategic competition, however they could be summarized in two broad areas. First encompasses some points that claim the West is wagging information war against Russia. Second includes researches who understand the full spectrum of vulnerabilities of contemporary security environment as well as these opportunities that come along with international interdependence. For them information warfare represents a form of political power and geopolitical instrument that allows a high level of manipulation and influence with a low probability of military confrontation. Here, the purpose is to promote specific political agenda where the competition is based on differences in ideology. As prominent pundit Dimitri Trenin insists that information warfare had become "*alongside geo-economics (sanctions and counter-sanctions), one of the principal battlefields in the new confrontation between Russia*

and the west." (Trenin, 2016) Certainly, it has one ultimate goal – to bring down public faith in the domestic political system by a combination of cyber-attacks and cynicism.

There are numerous ways to achieve this goal and they embrace many diverse channels for this. Let's consider some possible examples. First, propaganda that is spread through regular media, state owned channels and prominent people has a potential to win support mainly with sets of relevant target messages. (Timofeev, 2016)In addition to this, propaganda may divide key participants in the social and state life by exploiting sentiment patterns, fears, identity status and beliefs. In the center of this approach stays combinations of messages that have to influence people's behavior. It is a form of external narrative influence that may increase the sense of insecurity, play with ethnical heritage, national pride and morality.

Second, researches in Russia fully comprehend the high importance of existing social-cyber eco-systems and networks for covert manipulation that may raise the strains on current debates and advance specific political agendas. Information becomes a strategic tool that considers an enormous upload of personal information and opinions into social profiles. Undeniably, business with its digital marketing technics has used big data analytics to discover patterns, relationships and dependences for target messaging to sell its products. In the area of strategic competition there is a well-understood window of opportunities that big data provides for behavioral classification of individuals and groups of people. Considering this a malicious state or non-state actor may remotely and undetectably exert influence over a large portion of people and control their behavior. In essence, a technology that has been used to boost sells and consumption of specific goods may be used to distantly "manipulating electoral behavior." (Ovchinsky, Larina, & Kulik, 2015)

Third, cyber-attacks. In fact, many Russian experts understand the importance of cyber space and all the opportunities that come from it. Some of them consider it as a tool to gain economic benefits by penetrating state borders and manipulating the internal political situation. It also provides options "*to bypass the media domination and superior military potential of the United States.*"Moreover, energy grid, transportation system and critical infrastructure are prone to serious disruption in their operations due to cyber-attacks. (Valdai Discussion Club, 2017)The result is difficult to predict but it could cause large scale of social strife, financial and economic loses. For instance, the head of Threat Intelligence Department, Group-IBO Dmitry Volkov claims that main cyber-threat is an attack of "*pro-state hackers on large financial structures for the purpose of subversion and sabotage*." (RIAC, 2017)Additionally, because of critical infrastructure profound dependence on cyber space a successful attack on it has a potential to damage decision-making process and strategic management of military forces and assets. Pavel Sharikov argues that cyber-weapons may disrupt the functionality of civilian and military systems and "*in the event of an armed confrontation, the key issue is to destroy command, control, and communications".* (Sharikov, 2013) In fact, cyber weapons are a form of force multiplier that changes the paradigm of strategic stability.

Others accept cyber space as an option to spread information anonymously or to disperse it under fake identity. There is no authority to verify the reliability of information as well as to distinguish rumors from story that is prepared by someone order. In this form information warfare may affect different groups including their daily life, their perceptions and attitudes towards other countries. (Alekseeva, 2017) In other words, unstoppable flow of diverse and distort information puts strategic leadership and population in a situation that challenges the concept of truth and creates a complex artificial environment.

Forth, the dramatic expansion of technologies and their application into everyday human operations has produced more networks of interconnected people and devices. Their proper functionality in greater extent depends on electromagnetic spectrum that provides a conduit for signals and commands. Indeed, the huge number of sensor and devices that need data to fulfill their mission creates operational vulnerabilities. The main problem goes with information that is needed for force management, decision making process, command and control. For example, any disruption of intelligence collection, disturbance in surveillance or interruption of navigation could significantly degrade freedom of action and limit the number of possible options. Also, jamming of communication channels could bring down entire command and control system and may inflict significant costs. This is well understood in Moscow where the Chief of the General Staff of Russian Forces claims that vital element for future success in war depends on the engagement of electronic warfare systems that have potential to fight with air-space capabilities, navigation systems, digital communications and precision weapons. (TACC, 2018)Therefore, success in the war in the electromagnetic spectrum is a necessary condition for wining in conflict.

According to Moscow, information war takes opportunities to advance specific interests from existing favorable conditions. In fact, the Russian President Vladimir Putin contemplates information war as a form of strategic threat to the national sovereignty and defense capabilities because the outside invasion into critical infrastructure, the financial system as well as a leak of documents might have extremely heavy results to the national security. (Первый канал, 2017) Moreover, the chief of the General Staff General Gerasimov anticipates that success in war requires achievement of total informational dominance. There are multiple ways to accomplish this including media outlets, social networks, as well as capabilities for informational-psychological and informational-technical impacts. (Герасимов , 2017)

Summarizing, on the conceptual level military and security experts in Russia consider information warfare as a critical requirement for victory in peace and war. They assume it may change the entire national context that offers additional opportunities and has a potential to advance economic and political interests. Additionally, it can create conditions that do not exist domestically or internationally where their achievement could positively impact moral and social stability. Moreover, Russia considers information warfare as the strategic instrument of influence that can penetrate and distress the entire political, social and military stability and security. It has a potential to blockade on the massive scale these vital elements of the national security establishment that provide services for population and functionality of governmental agencies. The ultimate goal is to gain and maintain

informational dominance through traditional media, social-cyber networks, cyber space and electromagnetic spectrum.

CONCLUSION

We consider that in the area of national security information warfare represent a serious strategic challenge and a formidable threat that has several characteristics. First, the general intent of information warfare is to advance geo-political objectives while avoiding direct military competition and war. Second, information warfare utilizes multiple capabilities or channels which includes regular media as television, printed outlets, radio; modern media – social networks, web pages, accounts, blogs, posts; cyber networks – critical infrastructure, customer services, banks, transportation system and communications and electromagnetic space – communication networks and electronic devices that distribute messages and commands through electromagnetic waves with different frequency or wavelength. Third, information warfare exploits all possible opportunities and vulnerabilities thatrely on diverse often contentious points of view of population, individual and group marginalization. It also takes advantage from the profound dependence on cyber and electromagnetic networks that deliver vital signals for services, command, control and synchronization.

These futures generally provide multiple ways to reshape national security and the concept of modern conflict. In fact, one of the main components is the potent to project a combination of soft and hard power that becomes a weapon of influence over population and control over decisions. It flows through traditional defense borders and blurs the line between rational and irrational choices and actions. With minimum cost and risk, the attacker may plan and conduct covert and overt offensive operations that transform and extend traditional state conflict. This combined proactive approach of aggressive strategic destabilization is a form of limited war, a concept of dominant power, which takes energy from degradation of capabilities, erosion of beliefs and moral; disruption in decision making potential and discord in society.

References

Alekseeva, O. (2017, December 6). *Olga Alekseeva: Information War Affects Ordinary People*. Retrieved March 26, 2018, from http://russiancouncil.ru/en/analytics-and-comments/interview/olga-alekseeva-information-war-affects-ordinary-people/?sphrase_id=7426921

Bessi, A., & Ferrara , E. (2016, November 11). *Social bots distort the 2016 U.S. Presidential election online discussion*. Retrieved March 21, 2018, from http://uncommonculture.org/ojs/index.php/fm/article/view/7090/5653

Dale, H. (2015, April 15). *Russia's "Weaponization" of Information Testimony Presented to the House Foreign Affairs Committee on April 15, 2015*. Retrieved March 18, 2018, from https://www.heritage.org/testimony/russias-weaponization-information

Department of Justice. (2018, February 2). *Case 1:18-cr-00032-DLF Document 1 Filed 02/16/18*. Retrieved April 5, 2018, from https://www.justice.gov/file/1035477/download

DOD Dictionary of Military and Associated Terms . (2018, February). Retrieved from http://www.jcs.mil/Doctrine/DOD-Terminology/

Downes, C. (2018). Strategic Blind-spots on cyber threats, Vectos and Campaigns. *The Cyber Defense Review*, 1-19.

EEAS. (2016, February 16). *EUMC Glossary of Acronyms and Definitions Revision 2015*. Retrieved from http://data.consilium.europa.eu/doc/document/ST-6186-2016-INIT/en/pdf

Freedman, L. (2017). *The Future of War A Hstory*. NewYork: PublicAffairs.

Gertz, B. (2017). *iWar: War and Peace in the Information Age*. New York: Threshold Editions.

Goolsby, R. (2013). *On Cybersecurity, Crowdsourcing, and Social Cyber-Attack*. Arlington: Office of Naval Research. Retrieved March 21, 2018, from http://www.dtic.mil/dtic/tr/fulltext/u2/a580185.pdf

Gray, C. S. (2016). *The Future of Strategy* (Kindle Edition ed.). Cambridge, UK: Polity Press.

Mahaffee, D. (2018, February 23). *We've Lost the Opening Info Battle against Russia; Let's Not Lose the War*. Retrieved March 20, 2018, from http://www.defenseone.com/ideas/2018/02/weve-lost-opening-info-battle-against-russia-lets-not-lose-war/146212/?oref=defenseone_today_nl

Mckew, M. K. (2017, June 11). *Forget Comey. The Real Story Is Russia's War on America*. Retrieved February 26, 2018, from https://www.politico.com/magazine/story/2017/06/11/forget-comey-the-real-story-is-russias-war-on-america-215245

NATO. (2017). *AAP-06 Edition 2017 NATO Glossary of Terms and Definitions*.

Office of the Director of National Intelligence. (2017, January 6). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Retrieved February 26, 2018, from https://assets.documentcloud.org/documents/3254239/Russia-Hacking-report.pdf

Ovchinsky, V. S., Larina, E. S., & Kulik, S. A. (2015). *Russia and the Challenges of the Digital Environment*. Moscow: Russian International Affairs Council.

RIAC. (2017, October 12). *Specialists on Cyber Security Encourage to Change Public and State Attitude towards Cybercrime*. Retrieved March 26, 2018, from http://russiancouncil.ru/en/news/specialists-on-cyber-security-encourage-to-change-public-and-state-attitude-towards-cybercrime/

Rothkopf, D. (2014). *National Insecurity - American Leadership in an Age of Fear*. New York: PublicAffairs.

Sharikov, P. (2013, September 3). *nformation Deterrence: Transformation of the Strategic Stability Paradigm*. Retrieved March 31, 2018, from http://russiancouncil.ru/en/analytics-and-comments/analytics/information-deterrence-transformation-of-the-strategic-stabi/

Stretch, C. (2016, October 31). *Hearing Before the United States Senate Commiteeon the Judiciary Subcommittee on Crime and Terrorism.* Retrieved March 21, 2018, from https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf

Stupples , D. (2015, November 26). *The next war will be an information war, and we're not ready for it*. Retrieved March 18, 2018, from http://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218

Timofeev, I. (2016, June 6). *Russia and the West: An Information War?* Retrieved March 25, 2018, from http://russiancouncil.ru/en/analytics-and-comments/analytics/informatsionnaya-voyna-za-bilet-v-proshloe/?sphrase_id=7426921

Torossian , R. (2016, May 31). *Russia Is Winning the Information War*. Retrieved March 20, 2018, from http://observer.com/2016/05/russia-is-winning-the-information-war/

Trenin, D. (2016, Seoptember 17). *Information is a potent weapon in the new cold*. Retrieved March 25, 2018, from https://www.theguardian.com/commentisfree/2016/sep/17/hacking-politics-us-russia

Valdai Discussion Club. (2017, December 11). *Cybersovereignity Will Become A Prerequisite for the Creation of a Global Convention on Security in Cyberspace*. Retrieved March 26, 2018, from http://valdaiclub.com/events/posts/articles/cybersovereignty-will-become-a-prerequisite-for-the-creation/?sphrase_id=284897

Weedon, J., Nuland, W., & Stamos, A. (2017, April 27). *Information Operations and Facebook*. Retrieved March 20, 2018, from https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

Yarger, H. R. (2006). Towards A Theory of Strategy: Art Lykke and the Army War College Strategy Model. In *Guide to National Security Policy and Strategy* (pp. 107-113). Carlisle, PA: U.S. Army War. Retrieved March 8, 2018, from http://www.au.af.mil/au/awc/awcgate/army-usawc/stratpap.htm

Герасимов , В. (2017, March 13). *Мир на гранях войны*. Retrieved April 1, 2018, from https://vpk-news.ru/articles/35591

Первый канал. (2017, October 26). *Владимир Путин провел заседание Совбеза, на котором обсуждалась информационная безопасность страны*. Retrieved April 1, 2018, from https://www.1tv.ru/news/2017-10-26/335150-vladimir_putin_provel_zasedanie_sovbeza_na_kotorom_obsuzhdalas_informatsionnaya_bezopasnost_strany

ТАСС. (2018, March 24). *Генштаб: особенностью конфликтов будущего станет применение роботов и космических средств*. Retrieved March 31, 2018, from http://tass.ru/armiya-i-opk/5062463

How to cite this article:

Monov, LB and Karev ML.2018, Information Warfare Conceptual Framework. *Int J Recent Sci Res.* 9(5), pp. 26859-26866. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0905.2139

****