ORIGINAL ARTICLE Received 24 July. 2018 Accepted 12 June. 2019

Open Access Journal
ISSN: 2333-0783

ACADEMIC JOURNAL OF ACCOUNTING AND ECONOMIC RESEARCHES

Vol. 8, Issue 3, 33-40, 2019

Academic Journal of Accounting and Economic Researches

ISSN: 2333-0783 (Online)
ISSN: 2375-7493 (Print)

ajaer.worldofresearches.cm

The Role of Cyberspace in Advancing the Coming Battles

Davood Rezaei*, Hamdolla Nasrollahi
University of Khatamolanbiya, Tehran, Iran.

A B S T R A C T

Cyber warfare is doing or preparing for military operations in accordance with the principles of information. Cyber warfare means to disrupt, if not destroy completely the information and communication systems that enemy relies on them to "know", that is, who is? Where is? Can do what at what time? Why fighting? What threats are top priority? And etc. In cyber warfare, we are trying to know everything about the enemy and at the same time let him not know anything about us. In other words, the main objective of cyber warfare is to disrupt the "balance of information and knowledge" for the benefit of the forces, especially if the "balance of combat power" does not exist. Therefore, cyber warfare can be managed by taking advantage of superior knowledge to compensate the weakness of capital and personnel and achieve a decisive victory. The main purpose of this article is to clarify the role of cyberspace in Air Force cyberspace capabilities in terms of offensive and defensive war in facing wars of the Islamic Republic of Iran.

Keywords: Cyberspace, Cyber Warfare, Virtual Networks, Cyber Threats, Cybernetics, Information Technology, Virtual Organization.

INTRODUCTION

Stunning advances in information technology and communications had a major impact on agriculture and industrial society of modern world and entered humanity into a new era of information and knowledge. Consequently, the war has also witnessed fundamental change that sometimes it is referred to revolution in military affairs(Blackbourne et al., 2012; Brun & Valensi, 2012).

Today we are witnessing the emergence of modern warfare that from different aspects has fundamental differences with previous wars. One of the most important emerging areas in military affairs that was born with human arrival of the information age is cyber warfare and information warfare that essentially has its own approaches, tools, strategies, tactics and results(Brun & Valensi, 2012; Palmer, 2014; Parrott, 2012).

Information War (IW) is a relatively new term that in recent years has entered the dictionary of military terminology. The concept of using information in war of course, has the long history(Gul & Pesendorfer, 2012). The emergence of the term "information war" and its growing importance probably has direct relationship with the information revolution(Pomerantsev, 2015).

* . Corresponding Author: Rezaei, D.

To cite this article: Rezaei, D., Nasrollahi, H. (2019). The Role of Cyberspace in Advancing the Coming Battles. *Academic Journal of Accounting and Economic Researches,* 8 (3), 33-40.

Cyberspace is a term that is much heard in the world of internet, media and communications.

The word "cyber" is derived from Greek word Cybernetics(Blackbourne et al., 2012) meaning steersman or guide. The term "cybernetics" has been used for the first time by mathematician named Norbert Wiener(Brun & Valensi, 2012) in his book titled "Cybernetics and control in the relationship between animal and machine" in 1948. Cybernetics is the study of science and the control of mechanisms in human, car (and computers) systems(McCamley, 2013).

Cyber is a prefix to describe a person, an object, an idea or a space that is related to the world of computer and information. Many compound words from this word such as cyberspace, cyber money, cyber citizen and etc. has been arisen during the development of the internet.

The term "cyberspace" is used for the first time by William Gibson writer of science fiction in a book "Noromenser" in 1984.

Cyber space means a set of inter-human communication through computer and telecommunications issues without considering the physical geography. An online system is an example of cyberspace which its users can communicate with each other via email. Unlike real space, cyberspace not require physical movements and all acts done just by pressing keys or mouse movements. Research questions were:

- What are the appropriate structures to manage cyber?
- What are the threats in the area of offensive and defensive cyber in the war of the future?
- What is the vulnerability of offensive and defensive networks against cyber threats like in the future wars?
- How should be an appropriate structure to address and reduce the threats of offensive and defensive cyber in the future wars?

Research hypotheses:

Given that this study intends to evaluate the network detection and cyber threats of offensive and defensive networks in future wars. Therefore, any hypothesis is not expected for this study. In summary, for the following reasons any hypothesis for this study which is analytical and exploratory does not exist:

(A) Objectives is consistent with hypothesis

(B) Objectives are the core of the research. Therefore, with answering to the objectives, the hypothesis will be answered too.

METHODOLOGY

The research method is descriptive. Because the researcher sought to describe the requirements and cyber structure. Based on the studies and research with mechanisms, the researcher will create and provide cyber structure with new network point of view.

Model of the modern warfare

When investigating the pattern of the future wars, the conceptual approach of such wars must be illustrated. Of course, It is essential explicitly determine the horizon of futurology before drawing the concept mapping. Because according to the many changes that occur in different fields of modern civilization, any prediction or estimation about the world in the decades ahead will be likely high error. For example, despite the astonishing development and penetration of the information and communication technology and the tangible consequences and the impacts of this technology on the entity and principles of war, Today, no expert is not able to correctly predict the repercussions and impacts of revolutionary advances in nanotechnology and biotechnology, that their Golden Age may be started from 2020 onwards, on the wars in the coming decades. As a

result, in this report, the future horizons will be continued up to 2015, and preferably is silent about distant horizons. New operational concepts that will be emerged in the near future depend on the relations and interactions of the key elements in the future wars.

In the past three seasons, three key theories about the evolution of military affairs in the world to were introduced. Although hypotheses and inductive methods of these theories are somewhat different, but with the review and implementation of these three theories, a common point can be found between all of them.

For example, in fourth generation warfare theory that is based on ideas or new technologies, weapons of direct guidance of energy, robotics and media operations, and ultimately terrorism have been introduced which they result in the concepts of classical warfare, robot war, psychological war, and asymmetric warfare.

Also, in third wave war theory that is raised more in information-oriented society in which accurate-guided weapons, robots and nonfatal technology, weapons of direct-guided energy, and computer viruses are its focus, concepts of cyber warfare, advanced classical war and robot war are emphasized .

Finally, from the fourth era war theory in two forms - *western styles* based on advanced technologies, accurate-guided weapons, information warfare, nonfatal weapons, robotic military units, energy-guider weapons and also *non-western style* based on terrorism is introduced, the concepts of modern classical warfare, cyber war, robot wars and asymmetric warfare can be extracted. In fact, all the three theories mentioned are directly or indirectly insist on the importance of five war concepts as follow[4]:

- advanced classical war (both conventional and unconventional)
- Robotic war
- Psychological warfare
- Cyber war
- Asymmetric warfare.

It should be noted that the asymmetric warfare in itself is not a form of distinctive war, but it should be an approach or a different look to the war operation. Indeed, in an asymmetric warfare, there is a considerable difference between the forces of the two sides. For this reason, according to the strengths and weaknesses of the attacker and the defender of all four types of conventional war such as advanced, robotic, psychological, and cyber can be used. In other words, asymmetric warfares are essentially involved methods that follow in the levels of concepts and principles of classical advanced warfare (with or without the use of weapons of mass destruction), psychological warfare, cyber warfare, and robotic war. It should be also noted that in current definitions provided for the asymmetric warfare, the imbalance of the power between parties involved is emphasized and primarily asymmetric operations are attributed to the poor.

However, if the definition of asymmetric warfare with respect to important features "disproportionate effect" (i.e. the achievement of the goals of non-strategic activities) is expanded, we see that choosing a different approach to the war does not necessarily achieve in the light of the balance of military power. So, if a strong side detect that can reach its strategic objective, namely the surrender of the enemy and destroying its will and fighting spirit by using asymmetric methods, certainly will resort to asymmetric approaches.

In future wars, as in previous wars, primarily fulfilling two fundamental objectives are on the agenda, as follows(Porter, 2013):

- surrendering of enemy
- destroying the enemy

These targets by itself are important for politicians and military commanders, and we cannot find any the reason or reasons for their prominence. While other military targets, which are known as targets some point or tool, are considered only to achieve these two fundamental objectives. For example, capturing enemy territory is one of the military purposes that follow due to surrendering or destroying of the enemy. Experiences derived from recent wars have shown that without the use of weapons of mass destruction and only through strategic bombardment and bombard cannot forced to surrender the determined enemy and supported by public. As a result, similar to the old days, ground forces determine the ultimate fate of the majority of future wars; that is, whose mission and main goal are to seizure and occupy the enemy territory.

Figure (1) shows interactions between different concepts of war with each other as well as with their construction i.e. the information and communication technology (ICT) technology(Gray, 2013).

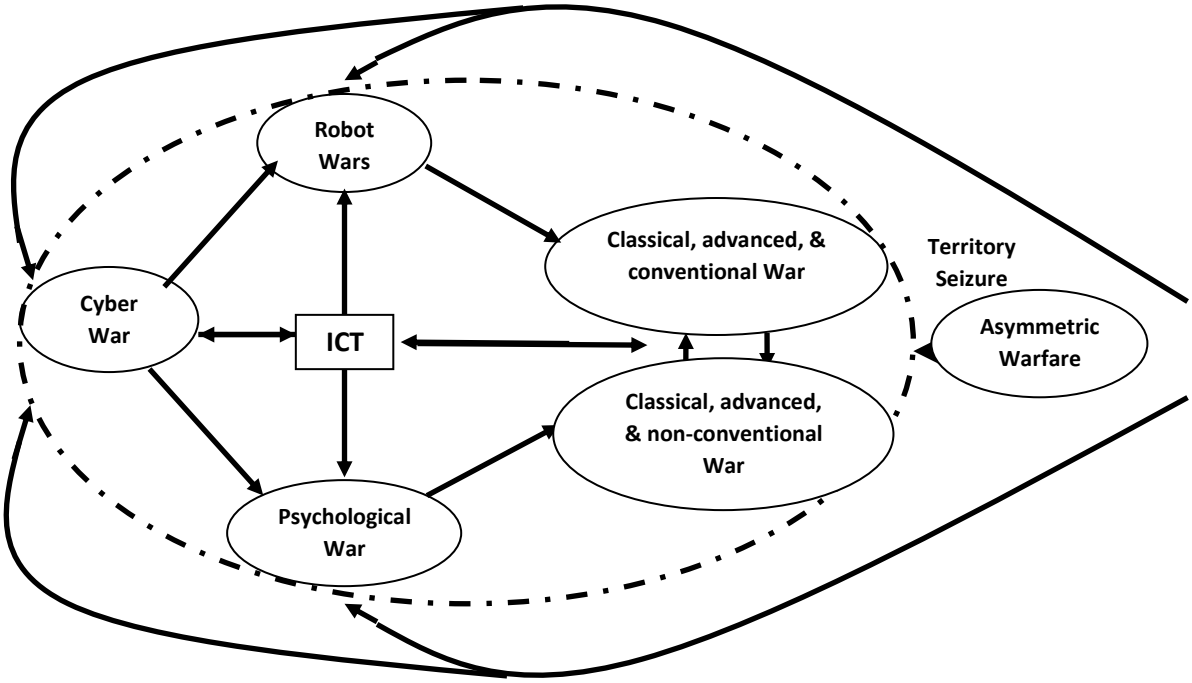

Figure 1. Model of modern warfare and the role of ICT

As you see, information and communication technology (ICT) system forms the core concepts of the future war. It is clear that without this main core, some new features and concepts in classical wars like accurate battle, away static invasion, guided weapons, "ever-awake eyes" and so on do not actually exist. In addition, the amazing development and penetration of ICT that makes the prospect of living in an interconnected "global village" closer to reality, in turn, has had a significant impact on the principles, methods, techniques and the effectiveness of psychological operations.

The two remaining robotic warfare and cyber warfare concepts are basically created as a result of advances in information and communication technologies and their importance in the coming years will be revealed more than ever. Arrows drawn between the concepts of war indicates the one-way and two-way impact (positive or negative). Concepts such as cyber warfare, robotic warfare, and psychological warfare all appear in the role of supporting the advanced classical warfare, and therefore, it is expected that the mentioned wars influence on the modern classical war. In some other cases, like the interaction between psychological warfare and cyber warfare, there is a one-way effect. In other words, cyber war influences on psychological war and

not vice versa. This logic of the effect regarding the relationship between the concepts of modern war and ICT is also true(Gray, 2013).

For example, any weakness or strength in vital infrastructure and software of the information and communication technology leads to the weakness or strength in different war concepts. As a result, the information and communication technology influences on all kinds of wars. But, Contrary to this relationship is necessarily not always the case. For example, psychological warfare has no definite impact on ICT system

RESULTS

A set of computer networks that exchanges data and information in local and wide-ranging nature and its scope of service is for mission and combat systems, is active in cyberspace. The structure of this network is in the context of open source systems, and therefore, it is considered as a new network.

Application Software: A set of programs that implements the application performance of a system in the form of a software such as personnel, logistics application system, and so on.

Cyber-defense: a set of actions that results in controlling virtual space of exchanged data and prevents the penetration of malware, viruses, and computer worms.

Malicious software: a group of programs that are designed to hurt the security. These include as follow:

A program that transfers confidential information to the outside.

A program that slows down the speed of processing system.

A program that clears the available information on the system.

A program that corrupts the available information on the system.

Virus: A computer virus is a piece of code that is unauthorized and unwanted copies itself into a larger program that is causing undesirable changes.

Computer worm: a standalone application that copies itself in the form reproduction from one computer to another on a network such as internet or an intranet.

Mission and combat net: A set of information network that is in the main platform of data exchange between command, control and intelligence related to defense affairs is called mission and combat net.

Cyber structure: A set of human factors, equipment and software that includes the nature of the cyberspace structure of the data exchange is called cyber structure.

Network monitoring: It refers to a set of actions and measures taken leads to monitor events and happenings in the field of network and cyber-attacks(Jordan et al., 2016).

Cyber threats: A set of malicious and effective factors that disrupts operation process of the network using various tools especially viruses, computer worms malicious software and so on and distorts the information of the network refers to as cyber threats.

Needed pattern to explain cyber warfare of Air Force in the offensive and defensive areas:

Offensive action:

It is an independent, qualitative, continuous, multi-valued variable that the researcher for analyzing it, investigated it with components such as virus projection, hack, crack, Trojan horses, electromagnetic bombs, and disturbing chip and explained their capabilities and effectiveness on future battles using documents and other sources with the method of qualitative analysis(Jordan et al., 2016).

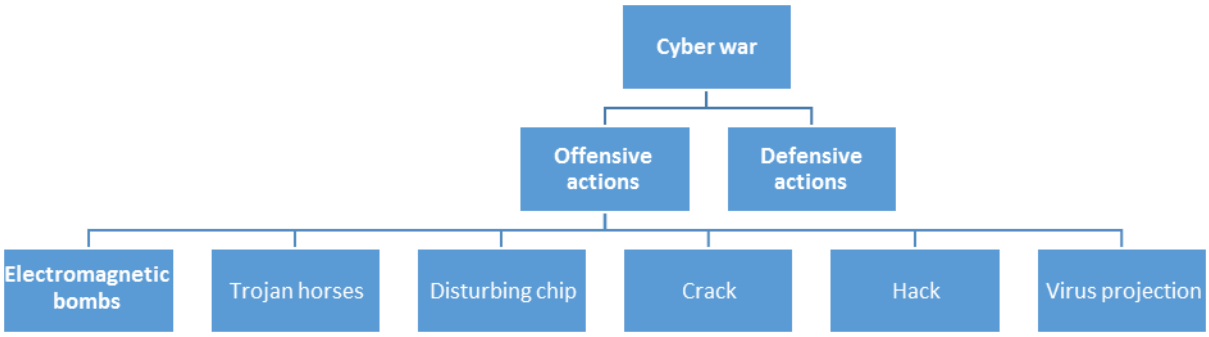

Figure 2. Offensive actions index

Defensive action:

Is an independent, qualitative, continuous, multi-valued variable that the researcher in this study for analyzing it, investigated it with components such as firewall, encryption, system traps, Faraday shield, infiltration detection, and system monitoring, and explained their capabilities and effectiveness on future battles using documents and other sources with the method of qualitative analysis(Gul & Pesendorfer, 2012).

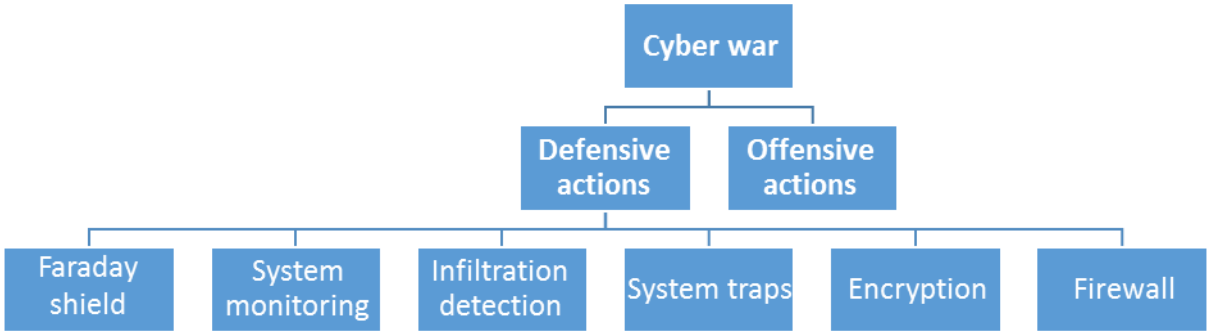

Figure 3. Defensive actions index

CONCLUSION

Certainly so far "no real experience" has not been happened in the context of cyber war or strategic information and therefore, evaluation of offensive and defensive capabilities is difficult.

There are considerable uncertainties and doubts about vulnerability of information infrastructures in all over the world especially in America. However, recent trends indicate that most countries have been a tendency toward less safe concepts of network design. US power arises as much as the weapons and military systems, it also depends on infrastructure of communications and civilian information. In the event of disruption or destruction of this infrastructure, the US economy is quickly stopped and perhaps even completely destroyed. Due to full dependence and reliance on computers, telecommunication systems, communications, and electronics, in the economy of a country like the US's, they cause weaknesses and new vulnerability in the body of the administration of this country(Floridi & Taddeo, 2014).

Less developed countries that do not much benefit from the infrastructures related to information are less vulnerable compared with developed countries that their lives primarily tied to

the ICT system. The evolution of information technology, are increasingly allowing the armed forces, to concentrate on integration of traditional forms of intelligence operations by help of comprehensive set of advanced information sources, surveillance and reconnaissance in a coordinated and synchronized intelligence operations. Developing the concept of "Global Information Grid" has caused the formation of network-centric environment that is necessary for this purpose. The network connects all network worldwide that links together the information capabilities, associated processes and people to manage and provide the information necessary for the forces, policy makers, and support staff. This network has been the bed of cyber operations and increased combat capabilities and also helped non-combat military operations to succeed. For example, since November 2002, America's Air Force pilots have made the latest version of a video game that can be connected to the computer network of America's Air Force via any typical computer that has a web browser and a special military software. Once connected to the network, they can guide the reconnaissance aircraft (drone) towards the goal, or demand for air strike. They can even design a flight path via a laptop connected to the Internet. Military use of the Internet is not considered strange. It must be remembered that invention of the Internet has taken place by the military, and especially America's Department of Defense. But, tools and weapons needed to carry out operation in this network (the Internet and cyberspace) are(Voigtländer & Voth, 2013):

1. Offensive tools such as computer viruses, Trojan horses, tools denial to service
2. Dual-use tools such as scanners of recognition of vulnerability in port, and network monitoring tools
3. Defensive tools such as encryption and firewalls

Offensive tools are used for "offensive computer network" against the enemy network and defensive tools are mainly used for protection against attack and eventually dual-use tools are used for offensive or defensive with regard to the intention of the user. Most recently, the software has been tested that can sneak into enemy computer networks to recognize what enemy radar systems reveal(Herd & Kriendler, 2013).

Offensive computer network is the offensive actions in order to disrupt, denial, degradation, or destruction of data recorded on computers and computer networks or computers and networks themselves. In offensive computer network, reliance is on signals interpreted in a data stream.

Much of the above actions has been to create the infrastructure of the cyber warfare and seriously not entered into the field of operational measures. But the relatively good abilities exist at the Informatics Center of Air Force with well-educated computer expert personnel having bachelor and master of art degrees and familiar to update computer science.

With respect to the past, it can be said that despite an appropriate platform (World Wide Web) and dependence of many developing extra-regional countries to it, implementation of operations, cyber offense by taking advantage of tools such as virus projection, Trojan horses, hacking and crack and the use of capable specialized personnel is possible in Air Force.

The countries that are passing the early stages of utilization of the information technology (IT), they are gradually moving from position of lack of relative vulnerability to position involving a degree of vulnerability. It is likely that in the near future, international studies about patterns, advantages, limitations, and conditions of information and cyber warfare, finally, most countries leading to the planning of defensive intelligence and they are required to improve the ability of information and computer network defense against its offenses especially from the United States of America. Hence, it is likely that an international market appears for designing and developing powerful tools of cyber defense that neutralizes most of the tools and techniques over time even within a day(Liles, Dietz, Rogers, & Larson, 2012).

The computer network defense includes measures that are taken for protection, monitoring analysis, detection and response to illegal activities in the systems and computer networks of the

armed forces. Defensive information warfare is measures that are taken to prevent, detect and deflect the enemy's direct or indirect actions against insider information systems. In computer network defense, the focus is on detecting and stopping the penetration of enemy agents.

Reviewing the process of network security actions in recent decades, it is seen that the firewall has been one of the first methods of network protection. Then, encryption, system traps, systems of detecting penetration, and virtual private networks came into existence. Nowadays, the public key infrastructure so-called PKI known as one of the best methods for network security practices.

REFERENCES

Blackbourne, L. H., Baer, D. G., Eastridge, B. J., Kheirabadi, B., Kragh Jr, J. F., Cap, A. P., . . . Butler, F. K. (2012). Military medical revolution: prehospital combat casualty care. *Journal of Trauma and Acute Care Surgery, 73*(6), S372-S377.

Brun, I., & Valensi, C. (2012). The Revolution in Military Affairs of the "Other Side". *Contemporary Military Innovation, 1642*, 107.

Floridi, L., & Taddeo, M. (2014). *The ethics of information warfare* (Vol. 14): Springer Science & Business Media.

Gray, C. S. (2013). *War, peace and international relations: an introduction to strategic history*: Routledge.

Gul, F., & Pesendorfer, W. (2012). The war of information. *The Review of Economic Studies, 79*(2), 707-734.

Herd, G. P., & Kriendler, J. (2013). *Understanding NATO in the 21st century: Alliance strategies, security and global governance*: Routledge.

Jordan, D., Kiras, J. D., Lonsdale, D. J., Speller, I., Tuck, C., & Walton, C. D. (2016). *Understanding modern warfare*: Cambridge University Press.

Liles, S., Dietz, J. E., Rogers, M., & Larson, D. (2012). *Applying traditional military principles to cyber warfare.* Paper presented at the Cyber conflict (CYCON), 2012 4th international conference on.

McCamley, N. (2013). *Cold War Secret Nuclear Bunker: The Passive Defence of the Western World During the Cold War* (Vol. 80): Pen and Sword.

Palmer, D. A. R. (2014). The NATO-Warsaw Pact Competition in the 1970s and 1980s: a Revolution in Military Affairs in the Making or the End of a Strategic Age? *Cold War History, 14*(4), 533-573.

Parrott, D. (2012). *The business of war: Military enterprise and military revolution in early modern Europe*: Cambridge University Press.

Pomerantsev, P. (2015). The Kremlin's Information War. *Journal of Democracy, 26*(4), 40-50.

Porter, P. (2013). *Sharing Power: Prospects for a US Concert-Balance Strategy (Enlarged Edition)*: Lulu. com.

Voigtländer, N., & Voth, H.-J. (2013). Gifts of Mars: Warfare and Europe's early rise to riches. *The Journal of Economic Perspectives, 27*(4), 165-186.