*Journal of Learning and Teaching in Digital Age, 2018,* ***3****(1)*, 12-20
ISSN:2458-8350 (online)
**Research Paper**

# Evolution of war and cyber-attacks in the concept of conventional warfare

Huseyin Kuru
Gazi University
yigit.cagatay04@gmail.com

Received 8 October 2017, Revised 6 December 2017, Accepted 6 December 2017

## ABSTRACT

Humanity have witnessed many confrontations of states whose interests challenge at some points and their struggle to neutralize problems in battlefield. While war was perceived as a way of eliminating deadlocks for some parties, some considered it as one of the international policy materials. The definition and content of conventional warfare have been subject to change for centuries, while the new weapons and technologies have been developed by human beings that it has brought constant change in the law of war and at the same time more lethal and devastating consequences. The struggle for superiority in international relations played an impulsive role in the development of weapons used in the battlefield. Countries have used their labor and financial resources to improve their military skills. Beginning with stones and sticks in the battlefield, this struggle has reached the point of using the next generation satellite controlled unmanned and armed aircrafts and having nuclear weapons has become more deterrent than using them. The struggle between strong countries and the limited countries in terms of technology and armed groups that do not have enough technology and skills completely changed the definition of conventional warfare. This fight has led *Asymmetric warfare* born which can turn commercial airline planes full of innocent people into a weapon like September-11 attacks. In this study, the historical development and the change in the content of the warfare were briefly explained and then cyber-attacks in the concept of the fourth generation warfare was analyzed taking into account of prominent attacks.

***Keywords:*** *Warfare, evolution of warfare, cyber warfare, cyber-attack, law of armed conflict, prominent cyber attacks*

## INTRODUCTION

The emergence of cyber-attacks has revived the anthems to define conventional warfare as well as the controversies on whether this kind of attacks are sort of warfare. As one of the most complex and diverse phenomena that guides the development of world history, word warfare is used as a rule, to express open and declared armed encounters between the opposing political forces within the state(s) (Aslan, 2008). At the beginning of the twentieth century the definition of conventional warfare that Lassa Openheim has made is one of the best examples. He pictured the war as; *"The confrontation of two or more countries to defeat the other by means of armed forces and winner's dictation of peace conditions."* (Oppenheim, 1906).

Yoram Dinstein has characterized the new model warfare as *"hostile physical and technical interaction of two or more states."* Denstein saw the situation that followed the declaration of war as the technical aspect of the war. He saw the physical aspect of the war as intention of making war for at least one part and for that purpose using of all national power components including armed forces (Dinstein, 1995). Although this definition is in the same group with modern ones, it has been loyal to the traditional rule that war would be only between states.

### Evolution of war

In history, mankind has begun to produce weapons using its own technology to fight better, this effort starting with arrow and sword has reached to nuclear weapons and the conquest of outer space (Gürcan, 2012). Figure 1. Shows the evolution of the war over time (Lind, Nightengale, Schmitt & Sutton, 1989).

***Correspondence to***: *Huseyin Kuru, Department of Forensic Computing, Institute of Information, Gazi University, Ankara, Turkey, E-mail: yigit.cagatay04@gmail.com*

**Figure 1.** The evolution of the concept of war over time

| 1. Phase | 2. Phase | 3. Phase | 4. Phase | 5. Phase |
|---|---|---|---|---|
| Wars before nation-states | **1. Generation war**<br>Classic wars (1648- 1830)<br>Top point: Napolyon Wars | **2. Generation war**<br>All together Industry Wars (1830-1918)<br>Top point: I. World War | **3. Generation war**<br>Maneuver Wars (1918-1948)<br>Top point:1991 Gulf War | **4. Generation war**<br>Unconventional Wars (From 1948 to our day especially aftermath of 11 September), Top point: US Afghanistan and Iraq Occupations. |

## First Generation Warfare

After a long period in the shadow of religious wars, the treaty of Westphalia, signed in 1648, points to a new turn. From this agreement, the period including the Napoleonic Wars shows the characteristics of these extensions. On first generation battlefield, armies had preferably large number of pianades with musket rifle their hands in the line arrangement. They tried to enhance maximum fire power on the front and they used technology and maneuverer at limited level. As a result of rifle and artillery shooting, the battlefields covered with a dense fog screen witnessed the artillery and cavalry could support the pianedes limitedly, and the soldiers who break the line order by being separated from one another are either killed by their friends or the enemy (Luvaas, 2001).

## Second Generation Warfare

The most important effects of the blessings of the industrial revolution and the application of the developing technology to the battlefield are no doubt machine guns and artillery which was getting more destructive than ever. Moreover, during this period, due to the increasing complexity of the services in the battlefield, auxiliary classes such as supplies, maintenance and personnel profounded as well as combat classes such as infantry, artillery and cavalry. With the introduction of the railroads in 1850, larger troops became portable, allowing strategic manoeuvring and shifting, while telegraphy enabled faster and more effective interaction. The application of steam engines and armour technology to army vessels has created a bigger and lethal naval force. In 1908 the planes were first used for military purposes, in 1914, exactly 6 years later, some of the major European states, such as Germany, Britain and France, each had more than 400 airplanes. In short, it was a period technology had determined war strategies (Hammes, 2004).

## Third Generation Warfare

After first world war(WW1) that German troops' victories by using "blitzkrieg" -storm- tactics, had built fundamentals of third generation warfare. Under the rule of this "blitzkrieg" tactics, all the military efforts were directed to weakest part of the enemy. After installing the power centre to this area, the enemy resistance was broken and after breaking enemy lines, the back bone of the foe was captured. After this siege the enemy was prevented from receiving logistic support from the back region. Dividing enemy in to parts could ensure his surrender or destroy. The use of the tank in the battlefield provided a very special multiplier effect. The tank combined manoeuvrability and superior fire power. Moreover, developments in torpedo and submarine technologies, the emergence of aircraft warships, Increase in range and characteristics of warplanes and developing sea and air manoeuvring tactics expanded the dimensions of battlefields to the fullest and deepest. In parallel with the developing technology, fighting planes, missile and even nuclear weapons, the concept of "total struggle" was born that targets economic facilities and civilians in the deep of the enemy country and the doctrine of "total war" inherited from First World War was reinforced (Gürcan, 2012).

**Fourth Generation Warfare**

For T.X.Hammes Fourth Generation Warfare is;

*“Evolved from upheaval, unfamiliar with conventional definitions of warfare, blurred lines between war and peace time, has no fronts and battlefield, wiping out the exact distinction between civilians and soldiers, fighting actors may be nonstarters as well as states, a kind of warfare that classical guerrilla and terrorism operations is revised and modernized of”*

In 1989, William S. Lind, Keith Nightengale, John Schmitt ve Joseph Sutton, wrote an article entitled -*The Changing Face of War: Towards the Fourth Generation War*- in the US Maritime Newspaper. İn that article they described 4th generation warfare as “*including asymmetric characteristics of military, para-military and civil efforts that distinction between war and peace periods is blurred, struggles stranded outside the designated battlefields, wiped out the exact distinction between civilians and fighting soldiers”* (Lind, Nightengale, Schmitt & Sutton, 1989).

The US army with defence spending of up to $ 700 billion a year (about half of the annual world defence spending) has created a huge "deterrent distance" with other states in the 3rd generation warfare. So there is no state that can stand against the US army in the conventional battlefield (Zenko, 2011). In order to close this "deterrence distance" at the level of the 3rd generation war and balance the power, many states that perceive the United States as a threat focus on the 4th generation warfare which provides less risky, less costly, more indirect and more promising solutions. David Kilcullen considers the US to be far ahead of other states on conventional warfare as the main reason why global terrorism is one of the hot topics of our time (CACI International, 2008).

<u>Changing the understanding of nation-state in battlefield</u>; In the new global security environment, “war monopoly as the highest type of political violence” is not in the hands of nation-states any more. One or more of the fighting sides are actors outside the state's regular armies. Now, warfare has become open to the effects of different non-state actors such as individuals, criminal organizations, extremist movements, ethnic violent trends. Furthermore, the concept of "security" became commercialized and seen as "service" with the use of the "Private Military Companies" which have tactical combat capabilities as we see the examples in the security field in Afghanistan and Iraq (Turcan & Ozpinar, 2009).

In the new global security environment, nation-states’ desire to wear down the woes by means of indirect ways rather than the conventional wars which are now costly to settle political issues, has led concept of "proxy wars" born. The best example of the “proxy wars” is the US-Iran relations. General Mohammed Caferi of the Republican Guard Guards Army claims that *"If there are those who think that the United States will solve his problems in Iraq, Afghanistan and Israel and then turn to Iran, they might be wrong. Because Iran will never allow the US to end its work in Iraq, Afghanistan and Israel”* (Kazemzadeh, 2007). In that case, the Iranian tactics are to determine the strategies that will enable the US to consume war resources and fighting wills in the streets of Baghdad and Lebanon and on the mountains of Afghanistan. Indeed, it is often mentioned that Iran is behind the overwhelming victory of Hezbollah against Israel in the 2006 Lebanon War (Cordesman, 2006).

<u>Transition from enemy-based to popular-based concept in warfare;</u> According to Gaula, the basic success criterion in the struggle is the degree of legitimacy of the socio-political order to be established as a result of the complete separation and isolation of the enemy from the innocent people. The center of the modern conflict environment is the support of the people (General Petraeus, 2010).

<u>Cyber warfare the new front of 4th generation warfare;</u> The most famous example of the cyber-attacks is the attack which started on April 27, 2007, targeting Estonia's financial centers, banks, parliament, ministries, security and transport infrastructure. For the first time in the history of humanity, a state had been subjected to a systematic, distributed attacks for three weeks and the belief that the 1.4 million Eastern European country has the power to establish security of citizens was rattled (Mansfield-Devine, 2012). The US Department of Defence who is seriously concerned about the cyber war and Russia, China

and Iran's developing significant offensive capabilities in the, due to its importance in order to ensure the doctrine and institutionalization in the US Army, the cyber space is defined as fifth battle field as well as land, air, sea and space (The Economist, 2010).

Ambiguity of line between war and peace time and unidentified victory conditions; In this type of warfare, the lines of the times of peace, crisis and battle, which are the stages of the conventional warfare, have become vague. For example, the 2008 Russia-Georgia conflict is a good example for this situation. However, the starting day of clashes is seen as 7-8 August Georgian attacks, in those days the border conflicts had already began. Although the parties officially finished, the conflicts continued for a while.

From conception of conquest (triumphalism) to man of peace; The 3rd Generation battles was carried out with the aim to conquest and victory as a result of the idea of killing before dying. The fourth generation battles have become more civilized and the goal has turned to win the people instead winning the the victory. Increasing importance of information operations; as a consequence of the Just War Theory media, civil society, political and economic capabilities have been used to break the judgments of masses and influence their thinking. Organizing military in tactical level; Another change brought by the fourth generation warfare is that the big and cumbersome army units like corps has been replaced by a smaller, professional, technologically advanced brigades (Gürcan, 2012).

This change-based concept of warfare has passed into a different phase with the September-11 attacks. After the attacks, terrorism became the most prominent element of the threat perceptions, making the concept of warfare more dispersed and vague (Raitasalo, 2005). The next day after the attacks, US President George Washington explained that the attacks were a war act againist US (Bush's Act of War Statement, 2001).

Cyber world is defined as fifth battle field as well as land, air, sea and space. The media, researchers, scientists and government officials often ring the cyber war bells and warn the public of imminent danger. In an article in the Wall Street Journal, it is claimed that nearly 50 countries are in a race for cyber weapons (Paletta, Yadron & Valentino-Devries, 2015). Two researchers at the Brooking Institute, P.W. Singer and A. Friedman draw attention to the danger of cyber arm race. Singer and Friedman have argued in their book titled *"cyber security and cyber war"* that about 20 countries have already developed advanced cyber weapons (Singer & Friedman, 2014).

## PROMINENT CYBER ATTACKS

### Likely state-backed cyber crime

Cybercrimes are committed in many ways but credit card and personal information stealing are the most prominent ones. The financial gain is the main purpose of these actions. Political and social motives are often the reasons that encourage cyber crimes. Activists often deface internet pages or perform distributed denial of service (DDoS) attacks for this purpose. As a result of DDOS attacks, requests are send at very high level that network capacity cannot endure so legitimate users are prevented from using that network as a result of exhausting its resources. Due to fact that this thesis generally deals with cyber acts that are behind or somehow supported by the states, actions of individual and private groups will not be examined here.

It is very hard to find out which state or person is the responsible or behind for a certain cyber-attack because of internet's unique nature. Even a state plays a role in a cybercrime, it generally chooses the way of denial (Carr, 2011). The targets of the cyber-attack examples investigated in this study are generally web sites of the governments. One of the common main characteristic of these attacks is that they are committed as a result of the support or permission of any state (Polityuk, 2016).

### 2007 Estonia cyber attacks

Estonia gained his independence in 1991 after the collapse of the Soviet Union. In the years following its independence, it has entered a rapid technological development. Estonia wasted no time in re-building itself as a modern, networked nation. It passed several stages of technological evolution, adopting e-services such as online banking with an enthusiasm and an adoption rate that many Western European nations could only watched with admiration. And it prospered the internet community supported a healthy economic performance. The population of Russian descent, corresponding as much as the quarter of the Estonian population, did not feel themselves Estonian and believed that the government is treating them as second class citizens (Mansfield-Devine, 2012).

This dissatisfaction of the Russian minority began to show itself through protests in 2006 and centred Russian soldier status. This statue of a Russian soldier was one of many erected across Europe by the Soviets resembling their fallen soldiers died in the war. But some of Estonia's Russian population viewed the monument as a symbol of their strong cultural links to Estonia's eastern neighbour but some Estonian citizens viewed it as an attack to their independence because they saw the Soviets not as liberators but as invaders. Estonian government took the decision to move the statue to another place and began working on the statue field on April 26, 2007, it was the time major demonstrations in the country began. On May 9, 2006, the protestors from this two different groups confronted in the area where the statue was located. The demonstrations that initially started peacefully turned into events of incineration and arson. But bigger problem was the cyber-attacks started in 27 April 2007. At first the authorities mostly saw these cyber-attacks as spontaneous reactions but later it was understood that the attacks were planned and coordinated (Mansfield-Devine, 2012).

Meanwhile, attacks on the communication infrastructure of Estonia completely stopped life in this little Baltic country. Government authorities and experts have blamed Russia for this digital attack, which is the first cyber-attack to target the national security of an individual country. The target of the attack is the media of the country, banks, communication infrastructure, business world and political organizations (Gamreklidze, 2014).

In 2007, cyber-attacks plagued all around Estonia. Although the country is currently the 153rd most populous in the world, the small Baltic state ranks 22nd out 144 on the Networked Readiness Index 2013. Estonia is traditionally assumed one of Europe's most *wired countries*. The cyber-attack was not a random event: it was in response to the relocation of a controversial Soviet war memorial. Estonia has been subjected to DDoS attacks targeting its financial and economic infrastructure for two weeks. What is the main purpose of the attacks? is it a virtual protest against the removing of the soldier-statue, an offensive tactic for provoking further conflict or the passing of a foreign actor in to the property of another? James Hendler, former Chief Scientist at the Defense Advanced Research Projects Agency, claimed that, "(they were) more like a cyber-riot than a military attack." (Caso, 2014).

These attacks continued at an accelerated pace and on May 9 reached the summit. On May 9, Russia's independence day, an estimated 85,000 captured computers participated in DDoS attacks (Whetham, 2016). Once the attacks started Estonian government has accused the Russian government immediately and claimed that Russia was the main responsible for the attacks. Nevertheless, the Estonian government has never proven the Russian's finger on the attacks (Rid, 2013).

## Cyber-attack causing physical damage

Almost all of the conventional armed conflicts result in physical destruction or loss of life. As of now, however, a very limited number of cyber-attacks have caused physical destruction or loss of life. In this section, Stuxnet one of the famous cyber-attacks and known to let destruction on property will be studied.

### **Stuxne**t

In June 2010, the Belarusian computer security company VirusBlokAda discovered a piece of malware and later named it as "Stuxnet". In the following months, it has been discovered that the Stuxnet virus is a highly advanced program targeting at certain types of computers and is spreading in certain countries like Iran (Symantec, 2010). According to the common opinion among researchers, Stuxnet virus's first and most important target is the nuclear facility in Natanz city of Iran. Experts claims that the virus was originated to target Simatic WinCC Step7 software, an industrial control system made by Siemens that was used to program controllers that drive motors, valves and switches in everything from food factories and automobile assembly lines to gas pipelines and water plants. If the malware's ultimate goal had been to destroy centrifuges in Iran and cripple the country's ability to produce a nuclear weapon, the consensus is that it failed. A conventional attack would have been much more deterrent though obviously much less secrecy or politically favorable. But if stuxnet purpose was only to retard and cause uncertainty in Iran's nuclear program, then it appeared to succeed but for a time (Zetter, 2011). Further analyzes showed that this unique cyber-attack caused limited damage due to limitations and defense mechanisms contained within the Stuxnet virus and could have had much greater impact without them (Langner, 2013). Stuxnet used the strategy of deceiving to hide the main reason why the centrifuges did not work properly from the Iranians. The software has used a method to read the status incorrectly to show that the centrals are functioning normally (Boothby, 2015).

In November 2013, security researcher Ralph Langner published a report on the Stuxnet virus and argued that the Stuxnet attack was the second phase of the operation and that in the first phase a secret version was aimed at increasing the pressure of centrifuges to provide extermination. According to Langer, the attackers struggled to increase stress on the centrifuge rotors in order to shorten their lifespan without causing suspicion of any foul process, rather than creating simultaneous destruction of hundreds of centuries which seems possible. As a result of such an approach, In 2009, attacks that are more famous and stealthy started. however, this time also, the attacker seems to have choosed an approach of somewhat less damage in a longer period of time compared to a simultaneous destruction of more centrifuges. Langner argues that without the less stealthy version, this virus would never have been discovered and he compared the attack with chinese version of water torture (Langner, 2013).

Stuxnet is the most complex malware that the world has ever seen. At least four new zero-day vulnerabilities, weakness in a system that have not been discovered before, were used in the same attack, sometimes even a single one is enough for a effective attack. Hackers place great importance on the zero-day vulnerability and would never disclose them unless unique times. Morover, Stuxnet has the ability to use digital signatures, which are required to enter the system and can only work with two original certificate keys that are apparently stolen from two very famous companies. This shows that Stuxnet virus has unlimited resources in its invention and that its creators are very determined to achieve their goals. In addition, Stuxnet has worked in all versions of Windows, including Windows 95, and had used a confidential account to pass Windows security processes (Singer & Friedman, 2014).

## Cyber-attack as part of conventional military operations

States can use cyber-attacks as a force multiplier in traditional military operations. One of them will be discussed in this part. These attacks, from their own perspective, are not aggressions that fall into the armed attack category, but they have crucial roles in facilitating access to the purpose of a traditional army operations and helping military purposes (Dinniss, 2012).

## Israel's Orchard Operation

Like most of the attacks in the cyber environment, the Israeli attack on Syria has also begun as a result of a human fault. A senior manager representing the Syrian government left his Laptop in the hotel room during a meeting in London. After he left, agents working for Mossad entered the room and placed a Trojan software on his computer. The Mossad agents, examining the pictures of the Syrian represent on his computer, find a picture of a blue-dressed Asian and an Arabian man shot in the middle of the desert. After a little research, they identified these two men. One of them was Chon Chibu, one of the leading names in North Korea's nuclear program, and the other was Syrian Atomic Energy Authority President Ibrahim Othman. When combined with other construction plans and documents such as the project of mines that can be processed, this picture showed that they were following the right man's computer and pursuing a nuclear plan. Israel government was right about to be worried at Syria might be pursuing a nuclear program (Follath & Stark, 2009).

### Technical Aspects of the Attacks

Although the technical details of cyber operations have weak relations with international law of armed conflict, it may be important to mention some general features of the attack in this section. Two prominent events, such as Estonia and Stuxnet, shed light on two very different styles of computer attacks. The Estonian attack can be likened in terms of technological level a town being occupied by thousands of soldiers, or by throwing thousands of bullets into the same target. In other words, this attack is technically very simple. On the other hand, Stuxnet attack can be seen as a special operation carried out by specially trained soldiers with detailed intelligence about the target. Thomas Rid noted that the cyber weapons are in a wide range of shapes, from those with ordinary but low potentials to those used in the Estonian attack, to those with special and high potentials like Stuxnet attack. The author compared ordinary cyber weapons to paintball guns. They have limited potential, they are easily available, getting hit is mostly visible but the effects of the attack are not especially permanent (Rid, 2013).

The Estonian internet infrastructure was hit with distributed denial of service (Ddos) attacks. The main goal of a denial of service attack is to exploit the bandwidth or the capacity of the target so that normal traffic cannot go through. A single user with a number of computers cannot do much damage by such attacks, which is why the more common variant is a *distributed* denial-of-service attack carried out by botnets. The botnet includes hundreds or thousands of malware-infected computers whose resources and bandwidth are controlled by the attacker, likely unbeknownst to the owner or user of the computer. This attack can also be coordinated at the same time, and those who want can participate in this attack. Such attacks require very little technic and resources. In the market you can find ready-made software that can do such attacks by simply entering the URL address or IP of the target (Valo, 2014). Such attacks do not require government resources or require very significant government support, Attackers often cause problems during the time that attacks are actively committed. In this period, the harmful heavy traffic prevents target system from being used. When traffic is heavy, it is possible to re-enter the site.

Malicious software components such as Stuxnet are usually programs that use software such as Java or Microsoft Word, or vulnerabilities -usually code errors- in the operating system like Windows. The attacker could use the current vulnerability to place malicious software on the target computer or network. After this, the software can infect other computers using the same vulnerabilities. A malicious software can use a malicious e-mail attachment, a website or USB drive to infect the computer. Malicious software can provide a botnet to the attacker to use the infected computer or access the web camera of the infected computer. Malicious software can delete all files on the computer or allow an attacker to send specific commands to a uranium centrifuge at a nuclear facility. In fact, the possibilities are practically limitless. It is also important to emphasize that when a vulnerability occurs, the patch is applied immediately and the vulnerability is removed (Greenberg, 2012).

## CONCLUSION

It is clear that there is a huge difference between the first definition of the war and the present one. The belief that the war needs to be between two independent states with the intention of fighting is now weakened by international terrorist attacks. Despite this, the states are striving to attribute the attacks to any country. After solving attribution problem, the right to self-defence comes into play. As seen in the technical analysis of the events that took place in the cyber environment, the complex structure of the internet, which derives attacks from cyber space in a traditional sense, makes it necessary to re-examine the traditional rules of conflict.

From a technical point of view, request countries to prevent harmful traffic passing through their networks would be very meaningless due to nature of the internet and traffic flow. When a user in Finland wants to enter a website that is hosted on a United Kingdom server, he has no chance to control which packages will go or in which way. At the first stage, the user's request may go from underwater to Helsinki to Sweden. depending on the network condition, it may be directed to the south to Estonia or St. Petersburg via cables underground. The data can go through many servers across the road, even if one of these servers is disconnected from the network, the data will be automatically forwarded to the server connected to another network. The user also has the chance at limited level to direct the traffic through the servers intentionally and hide the source of the traffic by encrypting this action along the way. Even if it is not impossible this makes it very difficult to find the source of the traffic (Rid, 2013).

It is impossible to secure computers hundred percent against cyber-attacks. As mentioned by Singer and Friedman in their book, "you cannot provide security unless you switch the plug off." (Singer & Friedman, 2014). The unique complexity of the software makes it possible to exploit vulnerabilities in practice. As it is said in this industry, "attacks always get better without worsening". This combination shows that efforts to exploit vulnerabilities and take countermeasures will continue increasingly. So the concept of cyberspace flexibility can be a new perspective, States and the private sector should aim to prepare as much as possible to alleviate the consequences of possible attacks, in addition to providing the security of the system (Avrupa Birliği, 2013).

## REFERENCES

Aslan, M. Y. (2008). Savaş hukukunun temel prensipleri. *Türkiye Barolar Birliği dergisi, 79*,470.

Boothby, W. H. (2015). Deception in the modern, cyber battlespace. In J. D. Ohlin, K. Govern and C. Finkelstein (Eds.), *Cyberwar: Law and ethics for virtual conflicts*. New York: Oxford University Press, 195-214.

CACI International. (2008). *Dealing with today's asymmetric threat to US and global security*. CACI International. 12.

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly Media, Inc., 176.

Caso, J. S. (2014, June). *The rules of engagement for cyber-warfare and the Tallinn Manual: A case study*. Paper Presented at the IEEE 4th Annual International Conference, Hong Kong, China.

Cordesman, A. (July 2006). Iran's Support of the Hezbollah in Lebanon, *Center for Strategic and International Studies*, 15.

Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. New York: Cambridge University Press, 265.

Dinstein, Y. (1995).*War, Agression and Self-Defense*, (2. Baskı) New York, Cambridge Univ. Press

Follath, E. and Stark, H. (2009). How Israel Destroyed Syria's Al Kibar Nuclear Reactor. *Spiegel Online*, 11.

Gamreklidze, E. (2014). Cyber security in developing countries, a digital divide issue: The case of Georgia. *Journal of International Communication*, *20*(2), 200-217.

General Petraeus'un 1 Ağustos 2010 tarihinde Afganistan Komutanı olarak yayınlandığı emir (2017), Retrieved from: http://www.isaf.nato.int/from-the-commander/from-the-commander/comisaf-s-counterinsurgency-guidance.html. 02.02.2017

Greenberg, A. (2012). Shopping for Zero-Days: A Price List for Hackers Secret Software Exploits, *Forbes*, Retrieved from: www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackerssecret-software-exploits/ 15.03.2017

European Union. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Retrieved from: www.ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 15.03.2017

Gürcan, M. (2012). Savaşın Evrimi ve Teorik Yaklaşımlar, A. Sandıklı(Ed.), *Teoriler ışığında Güvenlik, savaş, barış ve Çatışma Çözümleri*, İstanbul, Bilgesam Yayınlar, 71-133

Hammes, T.X. (2004). *The Sling and the Stone: On War in the 21st Century*, St. Paul: MN Zenith Press, 321.

Kazemzadeh, M. (2007). Ahmedinejad's Foreign Policy, *Comparative Studies of South Asia, Africa and the Middle East*, *27*(2), 446.

Langner, R. (2013). To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve, Retrieved from: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge, 19.12.2017.

Lind, W.S., Nightengale, K., K. Schmitt J. F. and Sutton J. W. (Ekim 1989). The Changing

Face of War: Into the Fourth Generation, *Marine Corps Gazette*, 22-26.

Lucas, G. R. (2016). Emerging norms for cyberwarfare. In F. Allhoff, A. Henschke and B. J. Strawser (Eds.), *Binary bullets: The ethics of cyberwarfare*. New York: Oxford University Press, 13-33.

Luvaas, J. (2001). *Napoleon On the Art of War* (New York: The Free Press), 99-120.

Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. *Network security*,*7*, 12-20.

Miller, S. (2016). Cyber-attacks and "dirty hands": Cyberwar, cybercrime, or covert political action? In F. Allhoff, A. Henschke and B. J. Strawser (Eds.), *Binary bullets: The ethics of cyberwarfare*. New York: Oxford University Press, 228-250.

Oppenheim, L. (1906). *International Law – A Treatise. Volume II: War and Neutrality* Longmans, Greenand Corporation, London, 56.

Paletta, D., Yadron, D. And Valentino-Devries, J. (October 2015). Cyberwar ignites a new arms race: Dozens of countries amass cyberweapons, reconfigure militaries to meet threat. *The Wall Street Journal*. Retrieved from: http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128. 21.02.2012

Polityuk, P. (2016). Ukraine sees Russian hand in cyber-attacks on power grid. *Reuters*, http://www.reuters.com/article/us-ukrainecybersecurity-idUSKCN0VL18E, 21.02.2017.

Raitasalo, J. (2005). The western war picture after the Cold War, in Jyri Raitasalo and Joonas Sipilä (eds), *Variable war*. National Defence University: Helsinki, 101–125.

Rid, T. (2013). Cyber war will not take place. *Journal of strategic studies*, *35*(1), 5-32.

Sanger, D. E. (2012). *Obama order sped up wave of cyberattacks against Iran. The New York Times*. Retrieved from: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-ofcyberattacks-against-iran.html?_r=0, 19.12.2017.

Singer, P. and Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University Press, 160-165.

Symantec(2010), Retrieved from www.symantec.com/security_response/ writeup.jsp?docid=2010-071400-3123-99. 18.02.2017.

Text of Bush's Act of War Statement (2001). BBC News, Retrieved at 03.02.2017from www.news.bbc.co.uk/2/hi/americas/1540544.stm

Turcan, M.& Ozpinar, N. (2009). “Who let the dogs out?”: A critique of the security for hire option in weak states. *Dynamics of Asymmetric Conflict*, *2*(3), 143-171.

Valo, J. (2014). *Cyber Attacks and the Use of Force in International Law*. Master Thesis, University of Helsinki, Faculty of Law, Helsinki, 12.

War in the Fifth Domain; Are the mouse and keyboard the new weapons of conflict? *The Economist* (2010). Retrieved from: http://www.economist.com/node/16478792. 19.02.2017

Whetham, D. (2016). Cyber Chevauchees: Cyber war can happen. In F. Allhoff, A. Henschke and B. J. Strawser (Eds.), *Binary bullets: The ethics of cyberwarfare*. New York: Oxford University Press, 75-88.

Zenko, M. (March-April 2011). The Future of War, *Foreign Policy*, 56-71.