THE NEW FACE OF THE WAR: CYBER WARFARE

Mehmet Emin ERENDOR[*]

Gürkan TAMER[**]

Abstract

With the development of the information technologies, computers and internet have played a crucial role in our life in the last decades. States, governments, NGO's, businesses, and other organizations take the advantages of these developments in terms of trade, economy, education

[*] PhD. Research Assistant, Department of Political science and International Relations-Çukurova University, can be accessed via mehmeterendor@gmail.com

[**] Undergrad, Department of Political science and International Relations-Çukurova University, Adana-Turkey.

and so on. Although technological developments enhance the ability of organizations to conduct activities in terms of cost-effective and efficient manner, it also has some disadvantages for the international community. Over the past decade, these technological developments have been used by some people, states or terrorist organizations to damage target states to improve their gains or impose their ideas or cut off the electrical power. Also, the Computer and internet was used a part of the war in Ukraine by Russia in 2015. In this study, the concept of cyber warfare will be analysed and its importance points and why states need to tackle with this situation will be explained.
Keywords: Cyber warfare, Cyber Disarming, Cyber Space, NATO, Estonia, Russia

Özet

Bilişim teknolojilerinin gelişmesiyle birlikte, bilgisayarlar ve İnternet geçtiğimiz on yıllarda hayatımızda önemli rol oynamıştır. Devletler, hükümetler, STK'lar, işletmeler ve diğer kuruluşlar, bu gelişmelerin avantajlarını ticaret, ekonomi, eğitim vb. gibi alanlar açısından kullandılar. Teknolojik gelişmeler, örgütlerin kabiliyetlerini etkin ve uygun maliyetli bir şekilde yürütme yeteneğini arttırmasına rağmen, aynı zamanda bu gelişmeler uluslararası topluluk için bazı dezavantajlara da sahiptir. Son on yılda, bu teknolojik gelişmeler, bazı insanlar, devletler veya terör örgütleri tarafından hedef ülkelere zarar vererek kazançlarını arttırmak veya fikirlerini dayatmak veya elektrik enerjisini kesmek için kullanılmıştır. Ayrıca, Bilgisayar ve İnternet, 2015 yılında Rusya'nın Ukrayna'daki savaşının bir parçası olarak da kullanıldı. Bu çalışmada, siber savaş kavramı analiz edilerek, önemi vurgulanacaktır ve devletlerin bu durumla niçin mücadele etmesi gerektiği açıklanacaktır.
Anahtar Kelimeler: Siber Savaş, Siber Silahsızlanma, Siber Uzay, NATO, Estonya, Rusya

INTRODUCTION

Although the identification of cyber weapons and the conceptualization of the cyber warfare are too difficult by the international community, these concepts have not commonly defined as it is the case for concept of terrorism. Besides, another problem of the international community is to generate disarmament regime (such as the International Atomic Energy Agency or the Chemical Weapons Prohibition and Prohibition Authority), but this requires a method of verification to achieve disarmament regimes involving cyber weapons (e.g. the NPT regime or the European Conventional Treaty). Although it is crucial to implement the rules of

disarmament, countries have continued to adopt new policies to improve their cyber capabilities. For example, cyber commanders are established, cyber-space and cyber instruments are used together with other elements of the war in the sense of common warfare.

In this article, our aim is to explain the basic principles of the cyber warfare and then analyse some possible effects of cyber warfare and cyber capabilities which can cause conflicts or wars in the international arena.

THE CONCEPT OF THE CYBER WAR

Cyber-attackers' capabilities not provide crucial manipulation and disinformation in conflicts also their capabilities create chaos in peace time. It has always been a critical target to penetrate masses' behaviours and perceptions through knowledge. During the Cold War, particularly during the periods of 1970s and 1980s, espionage was one of the most important influencing political tool which was used by the Soviet Union's intelligence agencies against the U.S. Nowadays, the espionage is using by states with using cyberspace and cyber space and cyber security, which have an important place today, can be portrayed as the access of important information through the use of computer and communication technologies. As a matter of fact, the work on the subject reveals that propaganda and manipulation activities of 'web robots' called 'bots' in social media are systematic, especially in the case of international crisis. There are also experts who interpret this as *'weaponizing information'*.[11]

It is not possible to evaluate the above-mentioned topics as a cyber-warfare. Obviously, in order to understand what the concept of cyber warfare is, it is necessary to first explain the truth 'what not'. Because, in popular usage of cyber warfare, any international competition activity using cyber instruments can be launched as a 'cyber war'. It would be unrealistic to evaluate cybercrime and even cyber espionage directly under the cyber warfare. Indeed, though it is possible that the world may be drifting into a "Cyber-Cold War" period with interventions in information, propaganda and even democratic election processes, but some scholars argued that there has not yet been a sizeable conflict that could be described as a "war" by military and military sciences in cyber-space. It would also be inconvenient for the concept of 'cyber warfare' to be used instead of 'cyber security', 'cyber-attack' or 'cyber espionage', and it is important to

[11] Sidney E. Dean Editor, Weaponizing Information: Propaganda Warfare in the 21st Century

provide terminological co-operation between the security science academy. It might be thought that cybernets are only made up of the internet. However, cyber-space also includes closed control systems that manage infrastructures and facilities that exist in physical dimensions beyond the internet, which is open to everyone and even encouraged. Due to the physical effects of the cigarette aggressors on the subject systems (e.g., general power interruptions or manipulation of SCADA systems in critical installations) can result in extensive loss of life and property. Here, the discussions about cyber warfare are coming to light because of these physical influences.

Finally, even if the above-mentioned problems are overcome, how will the collateral damage can be measured in spite of the inevitable, or when a cyber-attack on military targets creates the expected consequences? Today, armed forces with intelligent ammunition and sophisticated combat networks can overcome such concerns with technological-intensive operations. However, for cyber weapons, such an advantage may not be the case for all cases.

Speaking of which, collapse of internet networks and services in a country will certainly cause damage to civilians (Ball, 2017), Again, due to the unique nature of the cyber weapons, it is difficult for the offensive side to anticipate the possible consequences of the military planners. Only the mentioned qualities cause initiatives similar to the weapons of mass destruction of cyber instruments or disarmament initiatives to conventional capabilities to come to an end.

THE CONTROL OF CYBER WEAPONS AND CYBER DISARMING

At this point, it is crucial to understand whether international relations and international law frameworks on disarmament and arms control can be extended to 'cyber weapons'. Because, how and which parameters of cyber weapons can be limited/constrained to stuck to a single structure. Will the context of the restriction of cyber weapons be more similar to nuclear weapons or conventional weapons? Will it move from a different requirement?

The disarmament and restraint regimes differ from each other in terms of their causes and consequences. Such regimes may limit weaponry in terms of quality and quantity (e.g. European Conventional Force Treaty), prohibit the use of certain kinds and qualities of weapons (e.g. the Ottawa Convention), limit the trial activities of some weapons (e.g. Partial Nuclear Testing Prohibition Treaty) or prevent the production and stockpiling of certain weapons (e.g. the Convention on the Prohibition of Chemical Weapons). All these regimes are different from

the law of armed conflict. The purpose of such regimes is not to regulate state behaviour during the wartime but rather to prevent conflict and climbing itself (Geers, 2017).
What constraints should be made regarding offensive cyber skills - if so - by what conditions and parameters? Regulations on disarmament and arms restraint are made to achieve certain categorical results. This includes motivations such as minimizing military imbalances among states, raising predictability, avoiding the development of new weapons as much as possible, restricting spending on arming, or preventing irreversible and grave damage in case of armed conflict. Of course, at this point, it is of great importance to identify what is the offensive (cyber) weapon and, if possible, to categorize it.

Some scholars believe that there are two main categories of 'cyber weapons': those that do not need direct access to target computer systems (e.g., viruses that span the internet), those that have direct access to target computer systems (e.g. cyber agents that can penetrate SCADA systems and generate indirect kinetic effects) in the category. According to this approach, the elements to be subject to a possible regime of disarmament or arms control will be identified in the second category.

In order for cyber weapons to be subject to any international control regime, it is important for military and political circles to consider them in the context of 'strategic weapons', such as weapons of mass destruction or ballistic missiles. Studies of the subject state that the first and most important condition for the evaluation of the cyber skills used for military purposes in the 'strategic arms' segment is the catastrophic damage to the critical national infrastructure of an individual country. Until now, there has been no concrete evidence that cyber weapons have developed a destructive equivalent to nuclear weapons, which could upset the existence of a state (Schmitt, 1999). On the other hand, such a threat is not negligible, especially for countries that are carrying critical national infrastructures and economies to computer networks. Moreover, while the nuclear weapons regime is based on the non-use of these weapons, cyber skills can be used even in peace situations. Moreover, a state that is under attack cannot detect the actor who is attacking its own sovereignty. There is almost no such a situation for a nuclear attack. Offensive cyber skills are therefore frequently referred by international community.

In the case of 'Attribution', that is to say the source of the attack, it will be more realistic to compare offensive cyber skills with biological weapons. Because in some cases it may take time for an under-threatened country to understand that the threat it is facing an epidemic or a

biological warfare activity. Moreover, just as some bio-agents can be concealed for a period of time due to their incubation time, then a cyber-agent can also go through an 'incubation-like' process in computer systems.

The site is based on dual-use technologies that can be exploited for civil and military purposes, such as 'cyber weapons', the same chemical and biological weapons. In addition, while nuclear weapons are now monopolized by states, terrorist trends by the last ISIS threat and Al-Qaeda groups show that chemical weapons can also be used by non-state groups. This is also another case for cyber weapons.

However, although disarmament and arms control regimes for chemical weapons are exemplified, there is still a significant legal challenge in limiting cyber weapons. Because malware can be used to harm a system, spyware can also be used for espionage activities to learn about system vulnerabilities or information and information. However, spyware is the subject, and then the destructive malicious software that might come after it. Duqu malware, which contributes to the famous Stuxnet software, is a good example in this context. More explicitly, if Stuxnet, whose implicit kinetic influence, is the subject of a cyber-disarmament agreement, where would it be to put Duqu malware in this context?

It should be underlined that the greatest challenge for experts in any control regime concerning cyber weapons is to determine whether the parties are non-compliance. It is clear that governments will not look forward to a verification regime that will scan computer systems. Thus, even if a consensus is reached on the restriction of a cyber-weapon, which does not have an international mechanism with regulatory and sanctioning power, or where the verification regime is absent or limited, the situation that will arise is very similar to the Convention on the Prohibition of Biological Weapons, i.e. the control mechanisms will be ineffective.

It should be emphasized that weapons restriction and disarmament regimes are based on political-military considerations as well as international legal considerations. For example, the strategic evaluations of the Russian Federation and the US no longer needed chemical weapons after the Cold War brought with them the Regulation on the Prohibition of Chemical Weapons and the control of related weapons. Therefore, the main parameter to monitor of such consensus is found in the important and rising cyber actors of the international community.

As a matter of fact, an attempt by the Russian Federation, the People's Republic of China, Tajikistan and Uzbekistan in the UN in 2011 did not reach the conclusion due to the different ideas of Washington and Moscow. What is noteworthy here is the concern that a cyber-control regime has been used by authoritarian states as a censorship tool for the Internet and the flow of information. Another issue is that actors, such as the United States, who hold the technological superiority, must refrain from limiting and controlling these abilities by international mechanisms. It is difficult to analyse the concrete steps of the cyber warfare capacity without the barrier being overcome. Of course, while the need to prevent a cyber-space, armed race is increasing day by day, the world's leading armed forces continue to adopt new cyber policies and cyber instruments - at varying speeds.

In this framework, cyber commandments are established in many countries, and cyber-space and cyber instruments are used together with other elements of the war in the sense of a common warfare. In 2013, the Turkish Armed Forces took an important step by transforming the Cyber Defense Center into a Cyber Command. The establishment of the subject-matter command, which functions under NATO standards, is an important development in terms of the development of the Capacity of Communication and Electronic Information Systems of the Armed Forces and the national cyber defence solutions (Sofaer, et.all, 2000).

Also, cyber skills and electronic warfare are inseparable military tasks today. In this context, the recent breakthroughs of the Turkish Armed Forces and the Turkish Defense Industry are striking. The protocol signed with ASELSAN at the beginning of 2017 aims to increase the electronic warfare abilities significantly during the three years period (Aselsan, 2017).

Turkey is still far away from cyber warfare. First of all, it is a critical necessity to establish mechanisms and concepts to ensure regular and effective cooperation of academia, public, private sector and think tanks related to the subject. Secondly, and more importantly, the fact that the controversial offensive cyber skills debate in the world is not being done in Turkey adequately demonstrates that a more intensive intellectual effort is needed in the direction of the development of cyber military modernization. Thirdly, the increase in air defence capacities, especially in the immediate vicinity of Turkey, shows that it is vital that cyber and electromagnetic capacitance is seriously developed and integrated into deep attack capabilities. In defence modernization, more comprehensive steps are needed in this direction. In addition to what is stated, it should be noted that the cyber catcher had a grey area under the battlefield.

It is critical that the coordination of cyber-electromagnetic military developments with the efforts made by various institutions in our country and the formation of the vision for the situations under the war zone are critical.

HOW TO DEFINE A LEGITIMATE TARGET?

Armed conflicts related to the execution of cyber warfare is an important in terms of the application of the international law, and the 'legitimate aim' is who and what will constitute. Throughout history, the separation of civilians and military personnel has been based on sharp parameters. The use of uniforms by soldiers and the fact that military facilities have distinctive signs have created the first sign of this. Again, throughout history, the 'war zone' phenomenon has allowed civilians and civilian settlements to be precisely separated from conflict zones. On the other hand, the distinction between civilian and military targets is increasingly blurred. The trends that have developed in particular with the Second World War show that there are serious difficulties in protecting civilians from military operations and therefore the difficulties in question have increased (Ganuza, Hernandez and Benavente, 2011). The conflicts of 21st century, a hybrid profile exhibiting warfare in the residential neighbourhood made the civilizations a direct environmental factor. When it comes to cyber warfare, it is very difficult to distinguish between civilian and military targets. In fact, some experts consider that cyber warfare is a threshold from which the distinction between civilian soldiers and soldiers will be totally absent during the history of the war.

The question needs to be answered at this point with a meaningful consensus by the international community as: is there any of the cyber-attacks which is to be considered as a cause of war? and can the military response be legitimate?

Many experts suspicious of this suggest that cyber-attacks have limited - yet - ability to damage, and that the damage centre of the damage is mostly economic targets or consequences and therefore cannot be considered in a purely military framework. Those who come to the issue more differently think that the indirect kinetic effects of cyber-attacks, such as general electricity interruptions, can be regarded as a weapon attack, which can lead to life loss and cause death and damage to life in a country. From the point of view, there will be little difference between the direct kinetic effect (for example, by destroying the electrical

infrastructure with ballistic effect) and the indirect kinetic effect between the electrical infrastructure and the offensive cyber skills.

Cyber war - or possible future cyber wars - is another obstacle for armed conflicts, which makes the concepts of sovereignty of the state connected to geography and geography meaningless at a certain level. International relations have an organic relationship between the sovereignty of modern states and political geographies and borders. On the other hand, the geography that the state will use the sovereignty rights to date has, naturally, been defined according to physical qualities such as airspace and territorial waters. So, can a virus that targets a computer network be considered to have violated the political sovereignty of a state geographically? Because Article 2 of the UN Convention bans actions for the territorial integrity of states, the territory of the country, and the sovereign rights and independence of these territories. In that case, can the cyber agent mentioned in the above example be considered as a violation of the relevant article of the UN Convention? If indeed cyber instruments - such as conventional arms and weapons of mass destruction - are perceived as a threat to the basic parameters of the sovereignty and independence of the UN Convention, the restriction of disarmament and arms to these instruments would be based on a sounder basis of the regime.

Another issue that is crucial to the handling of cyber warfare as a military issue is the creation of doctrine. Because, in the literature, military doctrine means "belief system" for a military force. Military doctrines determine how the forces of the armed forces will fight, how they will perceive the environment of war and operation, the codes of enterprise and strategic culture, concepts and concepts. In this framework, military doctrines are prepared to respond to technical, tactical, operational, strategic questions and to cooperate with tens of thousands of staff to think and act.

If NATO is to be described as an operational environment with cryptic, space-based military functions, NATO has finally taken such a step - what elements would it contain as a cyber-warfare doctrine? The question we ask here goes beyond the different perspectives of different countries towards cyber warfare. Almost every national security document in the world has to make a threat definition and order. So, whichever country is prepared, the preparation of a cyber-warfare has to include some elements of the essence.

The studies in the literature focus on three main points in this respect. The first is related to how the perpetrator of the cyber-attack will be found and how it will be perceived (attribution problem). Because, at present, many states use surrogate groups for cyber-attacks. At this point,

it is very important to determine who to respond to in response to a cyber-attack. To give a more striking example for Turkish readers, at the end of 1990s, the Republic of Turkey has developed a new concept in the struggle with the PKK terrorist organization, focusing on the issue of 'deputy war', and on the Syrian Baath regime led by Hafız Asad, expressing his right to self-defence, directly putting pressure through the threat of war. In the 21st century, it is a very critical point that any state that is exposed to a cyber-attack by proxy will react to the sponsor state, whether it is a non-state proxy element or a cyber-attack.

Secondly, it is a matter that a cyber-warfare doctrine should absolutely address, how to do 'damage detection' about the consequences of a cyber-attack and how to assess the damage of a 'casualty' that an offensive cyber intervention gives to the enemy. At this point, measuring indirect effects is the greatest challenge.

Thirdly, and finally, taking into account the principle of proportionality, how and with which instruments a cyber-attack will be responded to is another key element in which a Cybercrime doctrine must respond. The point is that a state will respond to cyber warfare threats in a comprehensive and holistic manner.

Despite the above, there is a serious challenge to define the cyber warfare in the context of modern international relations and armed conflicts. Almost all the cyber-attacks are happening under the battlefield, and there are serious problems with their association with the offensive state. Experts who bring a holistic viewpoint to the cyber warfare and suggest that this new phenomenon should not be considered separately from the other elements of the warfare indicate that the cyber-attack and cyber warfare situations will not be limited to the cyber dimension due to the electromagnetic spectrum and will spread to the physical geographical dimensions. The most important argument of this hypothesis is that Russia has recently used and is currently using cyberspace as part of its overall escalation strategy in its interventions towards the former Soviet geography (lastly in Ukraine). In this context, attention is drawn to Moscow's' preparing the 'war zone' for special and covert operations, first with cyberspace.

Another noteworthy aspect of cyber warfare conceptualization is that there may be different approaches to the concepts of cyber war and cyber conflict. At this point, the main criticism of experts on the idea of cyber warfare is that all the cyber activities carried out in military or military-governmental institutions are regarded as a war effort. According to this

understanding, instead of treating cyber warfare as a separate element, it is necessary to understand that war for all organizations of armed forces based on computer and network technologies is 'cybersized' with every dimension. According to this understanding, the painting that emerges as the result of interaction with the physical four dimensions of the cyber-size (black-air-sea / ocean-space) shows that the armed cliché is gradually becoming "cyber".

CYBER WAR AND MILITARY ALLIANCES: NATO CASE

War is not just military technology and technology, it is an important element of international law and international relations. If Cyber is to be mentioned in words, it is also necessary to analyse the frame of the military options, such as the right to self-defence within the scope of the UN Convention, as well as military alliances and casus foederis against cyber-attacks, is required. Article 5 of NATO's founding treaty (Washington Treaty or North Atlantic Treaty) is one of the most concrete and dissuasive examples of what is now casus-foederis .

Is it possible for NATO to operate the 5th item in the face of an attack on one of the allied member states? As a result of 2014 Wales and finally the 2016 Warsaw summit, the North Atlantic Alliance today officially states that the cyber defence is part of NATO's collective defence mandate. Moreover, NATO emphasizes that international law can be applied to include cyber-space . Finally, the fact that cyber-space is an operational area at the Warsaw Summit gives an important idea about the political-military direction of the alliance's cyber skills.

NATO Secretary-General Jens Stoltenberg said in an interview at the press conference of the Defence Ministers in 2016 that the Der Spiegel correspondent would be able to trigger the collective defence clause in question against the question of whether the 5th article could be operated against a cheater attack on one or more members of the alliance, He replied that there was no obligation to operate the 5th article (Arimatsu, 2012). Indeed, it can be said that this 'vague' approach reveals both the process of adaptation of the alliance against cyber threats and the choice of flexibility in response options. It is frightening for the international community that the environment of cigarette conflict, which is still in its infancy, is causing a climb involving conventional and even nuclear weapons. As a matter of fact, Secretary General Stoltenberg said that the Russian Federation's intervention in the US presidential elections, which is one of the questions raised during the above-mentioned press conference, indicates that NATO's cyber skills do not target any country, and that the word 'Russia' preferred.

Nevertheless, the views gained in the latest Cyber Conference (CyCon 2017) organized by NATO's Centre for Civil Defence Excellence (Tallinn - Estonia) will leave open the way for Article 5 in case of a cyber-attack-like attack in Estonia that took place in 2007 it would be a much more rigorous response. Even at the level of diplomatic rhetoric, even in the face of cyber threats and taking an event as a scale, the imposition of a collective defence item gives an important idea about the future of NATO and cyber warfare. Of course, the views and analyses produced by the centres of excellence are not binding for the North Atlantic Alliance. However, it should not be forgotten that the analytical inputs mentioned may have serious consequences in some cases on the aspects of the North Atlantic Council and the elites who manage the NATO member countries.

GEOPOLITICAL CHARACTERISTICS OF THE CYBER-SPACE

Cyber-space has a sizeable impact on societies that cannot be compared to other dimensions of the warfare. Moreover, contrary to other known dimensions of warfare, cyber space is much faster than other dimensions, as cyber space cannot be physically controlled by a single state. More importantly, as the technological capacity of an actor increases, the land-sea-air-space systems and platforms become more dependent on cyberspace. Therefore, a weakness in cyber-space could lead to serious negative consequences for other dimensions, especially in terms of developed states.

The cyber-space is essentially 'in one form' in the other four dimensions of the warfare. More precisely, for example, the information transmissions from the sensors of war vessels cruising at sea or from airborne platforms and the data complexes stationed on the land are elements complementing cyber-space. There is a special relationship between space, the fourth dimension of warfare, and cyber space. Both dimensions are directly related to telecommunication and network technologies. In addition, operations performed in space are dependent on the capabilities of the cyber-space, operations performed on the cyber-space, and cyber electromagnetic activities are also dependent on support from the space dimension.

From a military point of view, cyber-space has important differences compared to other dimensions of land-air-sea-space quadrants. First of all, cyber-space, contrary to the historical and natural dimensions of war, is not qualified to be defined by known laws of physics. Of

course, the warfare also has social and political consequences of events that are of a physical nature. However, the kinetic effects of events in the field of warfare (eg, the shooting of a ballistic missile head with a target in the air, the shooting of an air platform with anti-aircraft fire, the shooting of an underwater platform of a submarine, the shooting of a military suit in orbit, shooting etc.) are also limited to the physically identifiable qualities of the physical warfare area or the fields. Many cyber-electromagnetic military activities can reach very complex and multi-dimensional domains of computation. For example, a computer virus can spread to countries that are not primarily targeted in various parts of the world, after affecting the systems of the target country. For this reason, it is very complicated to calculate the 'effective range' or the probability of undesired damage in cyber-space, as stated in the international legal review. Because cyber-space is a domain created for the use of information, for inter-human interaction, and for intercommunication. The field continues to exist together with the electromagnetic spectrum through telecommunication systems. More precisely, the mentioned telecommunication systems use the electromagnetic spectrum to form cyber-space by forming a global network.

Of course, due to the above-mentioned original qualities, the deterrence of cyber-space is also a difficult subject to understand from a traditional point of view. In particular, the basic components of the Cold War theories of deterrence, such as defence capabilities, credibility of threats, and the effective transmission of military-political messages, have to change for today's cyber parameters.

CYBER WARFARE'S FUTURE

Especially in the recent period, the revolutionary advances in electronic network-based communication have led to similar developments in battle networks. During the First World War, the use of telephone and radio lines to communicate with sea and land elements at long distances is regarded as the first battle network by some experts. Modern combat networks consist of command-control systems, target detection sensors & other discovery-surveillance-intelligence facilities, weapons systems and platforms, and electronic communication-based communication capabilities that connect all these elements together. The electronic revolution in communication facilities and capabilities has brought about significant changes in the understanding of military geography. In the first period when the 'human' began to fight as a species, the distance between the centre of administration and the elements of combat was to be the distance that the human voice could or could see. Today, as this distance has reached a

revolutionary point, network-cantered warfare also recognizes the possibility of engaging in weapons systems with targets that they cannot detect under normal conditions. Therefore, it is stated that battle networks competition has been experienced especially with the increasing speed from the Second World War, and this trend will continue to rise with great acceleration in the coming period (Geers, 2010).

In the age of cyber skills, such as the acquisition of information superiority, which is the basic principle of the network-based war, sharing information among friendly associations participating in the war and taking the common situational awareness to the top, out of the linear plane of the operation and effective use of synchronization. Moreover, the acquisition of knowledge superiority, that is to share with the friendly forces the most accurate and maximum information available on the battlefield in the fastest possible way, is to make the enemy as deprived of the same possibilities as possible, becoming a more important force multiplier in the cyber world.
As will be shown below, the network-based harness components show a great acceleration both quantitatively and technologically.

A study by the Defense Industry giant Raytheon has shown that among the technological trends that will determine in the future's war and in the third 'offset strategy' of the USA, the main artificial intelligence, innovations that will raise human-machine interaction, intelligent production technologies, micro- drones, weapons, cyber warfare, small & smart ammunition, and atomic particles.

Developments in the field of computer and robotic technology show that the future of automated systems in warfare environment will leave its place with autonomous systems. Unlike autonomous systems, autonomous systems will operate with a range of behavior options and state analyzes, rather than a single behavioral pattern. In this case, it will be an important part of both the strategic and military-ethical issues in the future of the war, although it is fundamentally a question of 'how robots think' based on software.

In sum, it is likely that developments in cyber skills will accelerate the transition of military strategies and concepts from platform-centric approaches to network-centric approaches. It is clear that the superiority of cyberspace in the future war and operation environment will naturally provide an advantageous position in information superiority and network-centered

capabilities. The 'Fruit Garden Operation *' - Mivtza Bustan * - which Israel carried out in 2007 with the aim of breaking the nuclear program of the Syrian Ba'th regime is a striking example of the use of cyber-electromagnetic activities as an attack in network-centered operations. Within the scope of the operation, al-Kibar was destroyed by the Israeli Air Force, a nuclear facility with strong suspicions that Syria was carried out with the help of North Korea and for military purposes. It is reported that some Israeli aircraft fuel tanks have also been left in Turkey.

Open-source publications on the subject indicate that Israeli F-15 and F-16s benefit from integrated intelligence, electronic warfare and cyber warfare capabilities to overcome the Syrian air defense complex. Accordingly, the series of projects that BAE Systems contracted and was called Suter was designed for tasks such as infiltrating enemy computer networks and manipulating radars, and began experiments at Nellis Air Base in early 2000. Suter is being conducted concurrently with the NCCT (Network-Centric Collaborative Targeting), an advanced, network-centric intelligence-discovery-surveillance-targeting precision ammunition-based offensive complex for the US Air Force.

Technical reviews of the topic reveal that Suter is more of a 'hacker' than a JAMMER, and it is stated that 'hacking' technologies and concepts related to computers have been combined with electronic espionage activities. It is also noted that Israel has used its 'Suter-like' systems since the Second Lebanon War in 2006 and benefited from these systems during the 2007 Fruit Garden Operation, as well as receiving instant data support from the US regarding the situation of Syrian air defence systems.

CONCLUSION

Although it seems certain that the cyber skills will be a serious game changer in the future of the war environment, it is not possible to say that a cyber-warfare has yet to be fully met by the armed conflicts law. Likewise, it is difficult to be optimistic about the establishment of a regulatory international mechanism for offensive cyber skills and the establishment of a verification regime. Because almost no country will be willing to open its own information and computer infrastructure to international control. In addition, some steps to date in the disarmament of cyberspace come from authoritarian regimes such as the Russian Federation and the People's Republic of China, causing serious doubts about the possibility that packages

on the Internet where individual freedoms are put in jeopardy under the name of trustworthy measures. In addition to those mentioned, it is unlikely that countries that have achieved significant advantages over technological capabilities, particularly in the United States, will be able to make an international bargain on the subject capabilities and capabilities.

On the other hand, it is important to establish an international legal norm and even an international mechanism for cyber-space conflicts. Serious problems can be encountered if these are not achieved, because it is considered that the cyber technology will reach 'critical mass' in the coming years. The 'critical mass' stage will then become a game-changing force multiplier in terms of the national power capacity of the developmental level countries in cyber-electromagnetic technologies, as well as the kinetic effects and secondary damage capacity will reach the limits of control.

It should be noted that not only 'weapons' but also 'targets' in this frame feed the trends outlined above. As the level of technological development increases, the economies of the countries, critical national infrastructure and social interactions become increasingly digital, becoming more dependent on computer networks and telecommunication facilities. Therefore, 'target options' of offensive cyber skills are expanding more and more every day. More crucially, facility infrastructure used for scientific research and civilian purposes, as well as for military programs in the CBRN field (chemical-biological-radiological-nuclear), is increasingly based more on SCADA systems. For this reason, it is a serious requirement to limit offensive cyber skills and attempt to establish norms for cyber-space conflict situations before the conclusion of the previously reported 'critical mass' phase.

In this period of dizzying development, it is useful to underline a few points as advice in the production of cybercrime for Turkish decision-makers. The first and most important parameter is the timing. Nations that are making the necessary investment in the technology competition today are expected to face a serious erosion in the national power capacities of the states that do not make investments in the years 2010, while the 2020s will overtake their investments in all areas of international competition (including peace and war periods) in the 2020s. Prerequisites for such investments are: scientific, innovative thinking with doctrine, human capital, inter-institutional coordination and coordination. Secondly, it is very important to be absolutely active in the cyber-space international legal normative process and to determine the diplomatic position. Because, the game rules in cyber-space are still in the process of being

determined. Thirdly, it is vital that Turkey focuses sensitively on the size of the cigarette in the risk and threat assessments that may arise either from other states or from terrorist organizations. In the national security analyzes mentioned, the main objective should be to minimize the strategic surprise factors that may arise from 'lack of imagination'. Finally, it is imperative that the academic resources and think-tanks in our country be encouraged to conduct research and debate on the fields of cyber conflict and cyber technology.

The wider framework of cyber conflicts, the narrower framework of cyber warfare, the basic finding of this work will be at the forefront of the other aspects of war and the nature of its partnership with technological developments. In this context, to focus on combinations such as cyber warfare and electronic warfare, cyber warfare and space technology, and even cyber warfare and biological warfare, can provide a more realistic vision of future predictions.

In today's and tomorrow's warfare environment, cyber-electromagnetic abilities will be critical in terms of network-centred joint operations against complex defences, especially called A2 / AD (Anti-Access / Area Denial). Therefore, this study will show that the centre of future wars will be shaped around C4ISR (military command-control-communication-intelligence-surveillance-exploration) networks, military satellite communications capabilities, cyber-electromagnetic facilities and capabilities and information- It foresees. It is likely that the main tasks will be to protect the subject systems from enemy penetration, and to stop the similar systems of the enemy.

Finally, it seems essential to develop a new paradigm, especially in the conflict situations that the West and NATO define in the classical sense 'under the battlefield'.

REFERENCES

Arimatsu, L. (2012). A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. *4th International Conference on Cyber Conflict*, Available at: https://ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf (Accessed at: 18/12/2017).

ASELSAN.(2017). Strategic Plan Summary. Availabe at: http://www.aselsan.com.tr/en-us/InvestorRelations/financial-data/Documents/Investor%20Presentations/ASELSANStrategicPlanSummary2017-2021.pdf (Accessed at: 18/12/2017).

Ball, Y. D. (2017). Protecting Falsehoods with a Bodyguard of Lies: Putin's Use of Information Warfare. *Research Paper NATO Defense College*, Available at: http://www.ndc.nato.int/news/news.php?icode=1017 (Accessed at: 18/12/2017).

Ganuza, N., Hernandez, A. and Benavente, D. (2011). An Introductory Study to Cyber Securıty in NEC. *CCDCOE*.

Geers, K. (2017).Cyberspace and the Changing Nature of Warfare. *Keynote Speech*, Available at: http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf (Accessed at: 18/12/2017).

Ottis, R. and Lorents, P. (2010). Cyberspace: Definition and Implications. *CCDCOE*.

Schmitt, M. N. (1999).Computer Network Attack And The Use Of Force In Internatıonal Law: Thoughts On A Normatıve Framework. *Columbia Journal of Transnational Law*, Vol. 37.

Sofaer, A. D., Goodman, S. E., Cuellar, M.F., Drozdova,E.A., Elliott, D.D., Grove, G.D., Lukasik, J.S.,Putnam, T.L., Wilson,G.D. (2000). A Proposal for An International Convention on Cyber Crime and Terrorism. Stanford University, Available at: http://cisac.fsi.stanford.edu/sites/default/files/sofaergoodman.pdf (Accessed at: 18/12/2017).