STUDY GUIDE:

NORTH ATLANTIC TREATY ORGANIZATION

CANKMUN'20

TABLE OF CONTENTS

LETTER FROM SECRETARY GENERAL

Dear Delegates,

It is my utmost pleasure to welcome you all to the CankMUN'20. I am happy to say that it is an honor for me to serve you as Secretary General in the first ever official conference of CankMUN.

I can assure you all that our conference will be unforgettable in every single way possible. Our organization Team, led by Ms. Sıla GÜLER, has put up so much effort to plan every single detail of the organization to give you the best experience possible.

It is my utmost pleasure to welcome you all to the CankMUN'20's North Atlantic Treathy Organization.

Our distinguished Under Secretary General Bersu CENGİZOĞLU has prepared this study guide for you to understand the concept of this committee as well as the questions to be adressed. I recommend you to read the Rules of Procedures of CankMUN'20 since it will be the main course of our procedures.

This committee is well thought and prepared. Get ready for the fun and the crisis all along the conference. There will be lots of surprises among the 3 days ahead of you

Both our organization team and academic team has been working so hard to make this experience unique and unforgettable.

Get ready to enjoy this committee to its finest. Lets ***#BeeInTheFuture*** to create a better future from now on.

Sincerely
Enzel Ege SARI
Secretary General of CankMUN'20

LETTER FROM UNDER-SECRETARY GENERAL

Distinguished Delegates,

I am honored to be your under-secretary general for this NATO committee and I am thrilled to work with our team to give you the best NATO experience possible.

In this committee we gave you two very important topics. I expect from you, to understand these issues in detail and to focus on important points and questions. When you read and understand the topics well, you will do the rest and you will have a committee experience with both fun and excitement. I also recommend you to be prepared for unexpected crisis. I hope that each delegate does their own research on this complex subject and reads this study guide carefully.

We expect serious conduct during the conference and hope that you will enjoy this experience fully. I wish all of you the best of luck!

If you have any questions, feel free to ask through email before the coference or during the conference.

BERSU CENGİZOĞLU
UNDER-SECRETARY GENERAL OF NATO

1.INTRODUCTION TO THE NORTH ATLANTIC TREATY ORGANIZATION

1.1 WHAT IS NATO?

The North Atlantic Treaty Organization also called the North Atlantic Alliance, is an intergovernmental military alliance between 29 North American and European countries. The organization implements the North Atlantic Treaty that was signed on 4 April 1949.

North Atlantic Treaty Organization is a military and political alliance of countries from Europe and North America. Its political aim is to create an opportunity for its member states to consult and cooperate on defence and security related issues, solve problems and prevent conflict, wheras its military aim is to resolve disputes in a peaceful way. NATO is committed peaceful resolution of disputes but it also has the military power to undertake crisis-management operations.

1.2 THE HISTORY OF NATO

On 4 March 1947 the Treaty of Dunkirk was signed by France and the United Kingdom as a *Treaty of Alliance and Mutual Assistance* in the event of a possible attack by Germany or the Soviet Union in the aftermath of World War II. In 1948, this alliance was expanded to include the Benelux countries, in the form of the Western Union, also referred to as the Brussels Treaty Organization (BTO), established by the Treaty of Brussels.Talks for a new military alliance which could also include North America resulted in the signature of the North Atlantic Treaty on 4 April 1949 by the member states of the Western Union plus the United States, Canada, Portugal, Italy, Norway, Denmark and Iceland.

1.3 THE MISSION AND PURPOSE OF NATO

NATO states its purpose as "to guarantee the freedom and security of its members through political and military means". As a political entity, NATO "promotes democratic values and enables members to consult and cooperate on defense and security-related issues to solve problems, build trust and, in the long run, prevent conflict". As a military entity, NATO exerts military power to manage crises when it is not possible to resolve a conflict through peaceful, diplomatic means. Its primary purpose was to deter Soviet expansion and spread of communism in the West, until the collapse of USSR in 1991. Since 1991, NATO alliance has focused on maintaining the underlying strategic cooperation between its member states to preserve peace and security across Europe, and to some extent Middle-East and North Africa. NATO has since assumed a more proactive role in the world stage, intervening in many varying capacities across different parts of the world, a recent example being the NATO led coalition against Libyan government in 2011.

1.4 REPRESENTATION IN NATO

Each member nation has an ambassador, or permanent representative that represents it and is supported by a national delegation which includes advisors and officials who represent the country in different NATO committees. NATO also meets on the heads of state and government, minister of foreign affairs, and minister of defence level. Military representatives who are chiefs of staff are permanently based at NATO heaquarters.

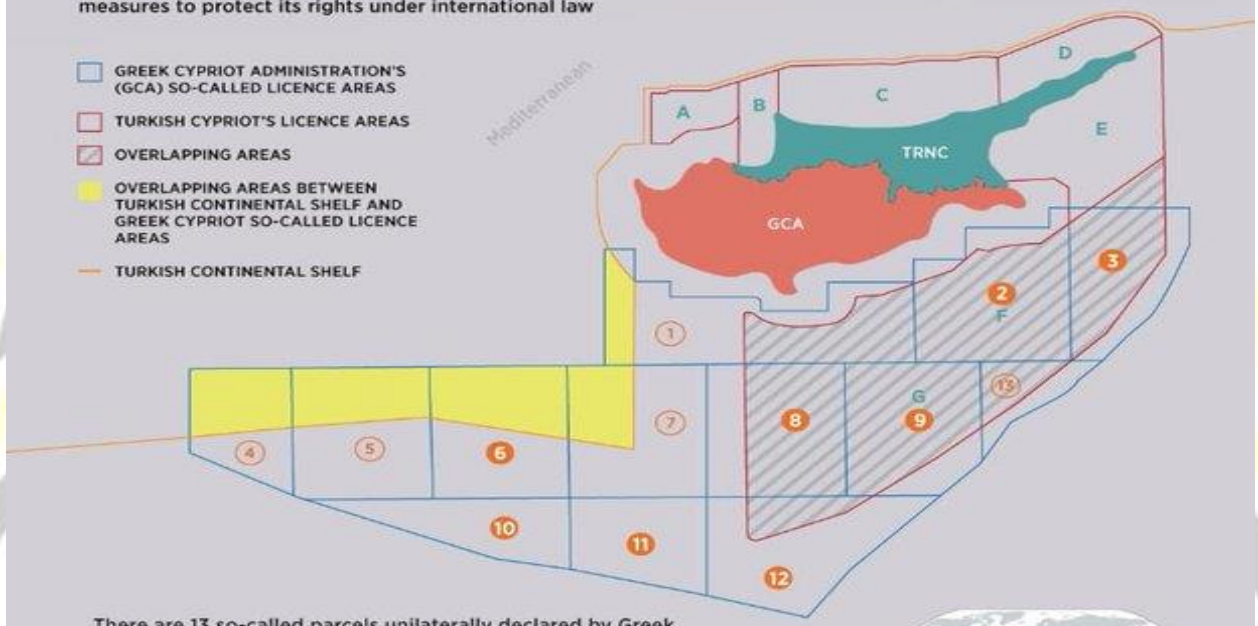
2.INTRODUCTION TO THE FIRST AGENDA: NATURAL GAS DRILLING SITUATION IN EAST MEDITERRANEAN

2.1 How Did The East Mediterranean crisis develop?

The 2018 Cyprus gas dispute is a diplomatic dispute involving the exclusive economic zone (EEZ) of the Republic of Cyprus (in partnership with Greece and Egypt) in the eastern Mediterranean, which began on February 6, 2018. The dispute followed remarks made by Turkey's foreign minister Mevlüt Çavuşoğlu, rejecting a 2003 Cypriot-Egyptian maritime border demarcation deal and announcing the Turkish government's intention to carry out gas exploration in the region. Tensions in the region further escalated on February 9, when the Turkish Navy blocked a drill ship operated by Italian oil company Eni S.p.A, licensed by the government of the Republic of Cyprus, from exploring gas reserves off the island. ÇAVUŞOĞLU (Turkey foreign affairs minister) said during his interview with the Greek newspaper Kathimerini that Turkish Cypriots have "undeniable rights" to the Cypriot EEZ. Egypt's Foreign Ministry reacted by warning Turkey not to contest the 2013 deal and Egyptian economic interests in the region, adding that any attempts to do so would be confronted. The Cypriot government officials have emphasised that any future benefits are for all Cypriots, including the Turkish Cypriots, but only after a comprehensive settlement of the Cyprus problem. On February 16, Eni CEO Claudio Descalzi stated that the Turkish blockade of its drill ship, Saipem 12000, was out of Eni's hands and that the issue was being discussed by involved parties. In November 2018, the partnership of the Cypriot government and US company ExxonMobil successfully began carrying out hydrocarbon exploration, escorted by US Navy ships, with Turkey remaining passive.

Turkey's stance in the Eastern Mediterranean is clear

Some countries, ignoring the rights of Turkey and the Turkish Republic of Northern Cyprus (TRNC) in the Eastern Mediterranean, try to unfairly claim its natural resources. But Turkey is taking measures to protect its rights under international law



There are 13 so-called parcels unilaterally declared by Greek Cypriots and contracted with international oil companies

Since Greek Cypriots do not represent the entire island, they do not have the right to continue off-shore activities unilaterally

10

In the 10th parcel, there is a partnership between US' **ExxonMobil and Qatar Petroleum**

12

Field 12 includes shares apportioned to **US' Noble Energy, Britain's BG, and Israel's Delek and Avner**

6 11 8

France's Total and Italy's Eni have equal shares of the 6th and 11th parcels while Eni alone has the 8th parcel

2 3 9

In the 2nd, 3rd and 9th parcels, **Italy's Eni and South Korea's Kogas** have joint licenses

Greek Cypriot effort to license out further areas contiues for the following so-called parcels:

- 1 1ST
- 4 4TH
- 5 5TH
- 7 7TH
- 13 13TH

10 11

There is no overlapping in the so-called **10th and 11th parcels**. Yet Turkish Cypriots claim shares in all so-called Greek parcels as they are the co-owners of the island

TURKEY WORKING TO PROTECT ITS OWN RIGHTS AND TRNC'S RIGHTS IN THE EASTERN MEDITERRANEAN

Turkey's seismic vessel **Barbaros Hayreddin Pasa, along with Yavuz drilling vessels**, started drilling and exploring the areas called **A, B, C, D, E, F and G, under TRNC licenses.**

The **Barbaros Hayreddin Pasa** started 2D and 3D seismic work in 2018.

Turkey's first drilling vessel **Fatih** began work 60 km west of the island of Cyprus in May under Turkish government's licences 2009-2012 in the Turkish continental shelf.

On June 20, the **Yavuz** drilling vessel left for its mission in the Eastern Mediterranean to operate in TRNC licence area

10.07.2019

Anadolu Agency

2.2 How did the natural gas search crisis off the Eastern Mediterranean - Cyprus coast begin, which country wants what?

Turkey's Fatih and Yavuz send the drill ship to Cyprus to open and the ship's Northern Cyprus authorization given regions where natural gas exploration to begin, the Greek Cypriot side, as well as Greece, the European Union, Egypt, has already met with Israel and the US response.

Southern Cyprus and Greece say drilling activities are a violation of Cyprus' exclusive economic zone.

The European Union supports Greece and Cyprus in this regard. European Council President Donald Tusk said in a statement this week that "the European Union is behind Cyprus. We call upon Turkey to be respectful of the sovereignty of the EU member states. Will continue to monitor closely the Council of Europe developments," he said.

Turkey says will not be suspended drilling operations.

2.3 WHAT CAUSES THE TENSION

The history of the increasing tension in the recent period dates back to the early 2000s, when the scientific predictions of rich natural gas resources in the Eastern Mediterranean began to emerge.

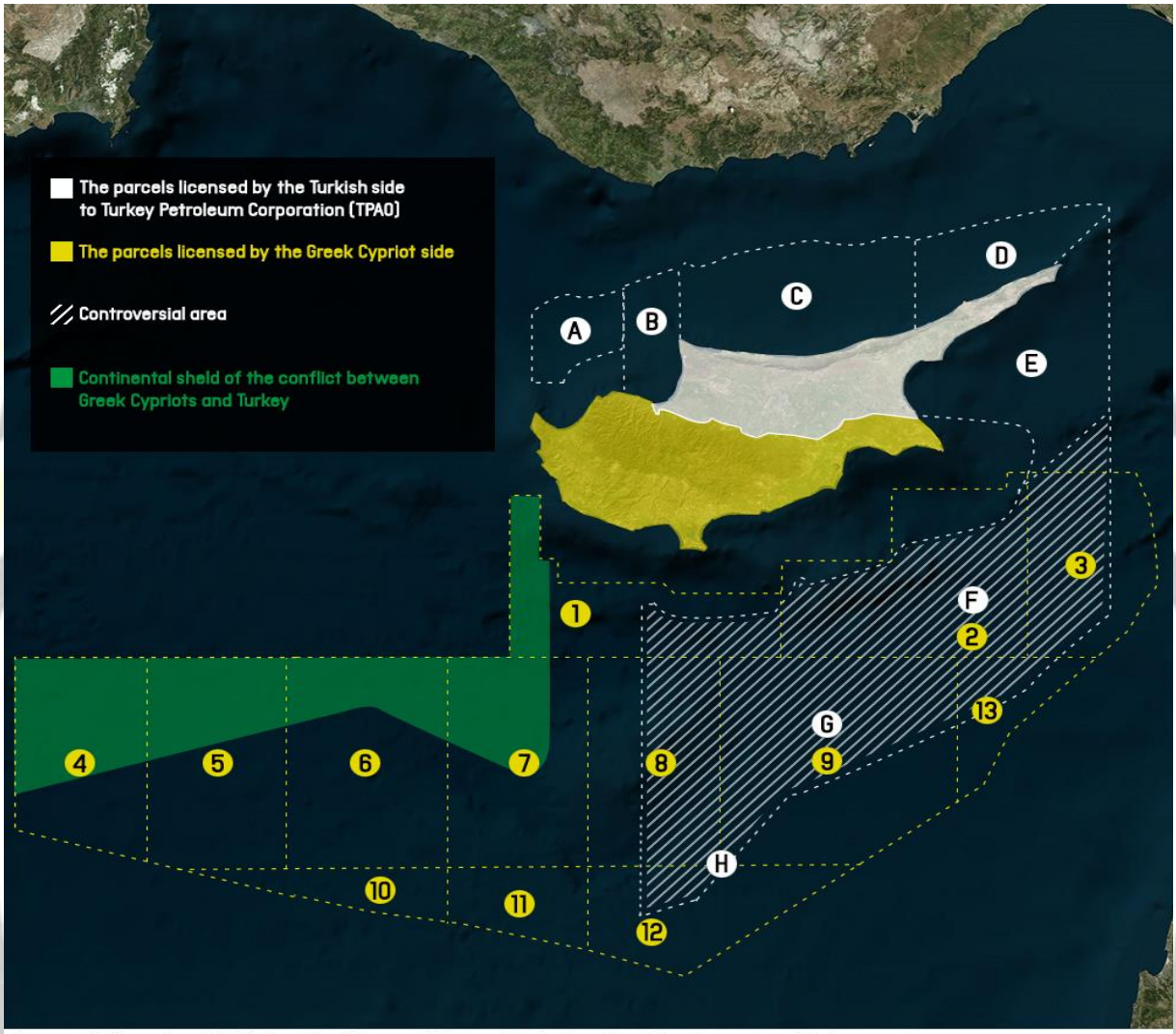
Since 2002, the Republic of Cyprus has entered into Exclusive Economic Zone (EEZ) agreements with Egypt, particularly Egypt, other coastal countries, Lebanon, Syria and Israel.

Turkey is the subject of these agreements on the grounds that Cyprus and Turkey violated the rights of Turkey's UN vehicle and was approved by the UN at its exclusive economic zone map.

Despite the objections of Turkey in Cyprus before the UN, declared at the beginning of 2007, 13 exploration areas and the major oil companies have passed the licensing phase. In return, Turkey, the Eastern Mediterranean region in its economic zone in the North of Cyprus in the island's north and east determine gave Turkey Petroleum Corporation (TPAO) exploration licenses.

Cyprus is one of the 13 plots, 4, 5, 6, and 7 of a portion of parcels (in figure 2) , Turkey's Turkey Petroleum Corporation (TPAO) intersects with the block that is licensed. Parcel no. 3

coincides with the privileged area that Northern Cyprus has given to Turkey Petroleum Corporation (TPAO).



2.4 HOW DID TENSION GROW?

The size of the tensions between Turkey and Cyprus, since 2010 the discovery of rich hydrocarbon deposits in the eastern Mediterranean and was further increased with the influx of large international energy companies to the region.

Noble and Exxon Mobil companies in the US, as well as Italian ENI and French Total companies continue their activities in the region within the framework of their agreements with Cyprus.

Exxon Mobil's search for natural gas in the parcel no. 10 on the southern part of Cyprus Island at the end of 2018 was a step that further increased the tension.

Cyprus was quick to respond to this move of Turkey. The first drilling ship in the Mediterranean Sea protection of Turkish warships issuing Fatih Turkey, began gas exploration activities on its continental shelf in the remaining region.

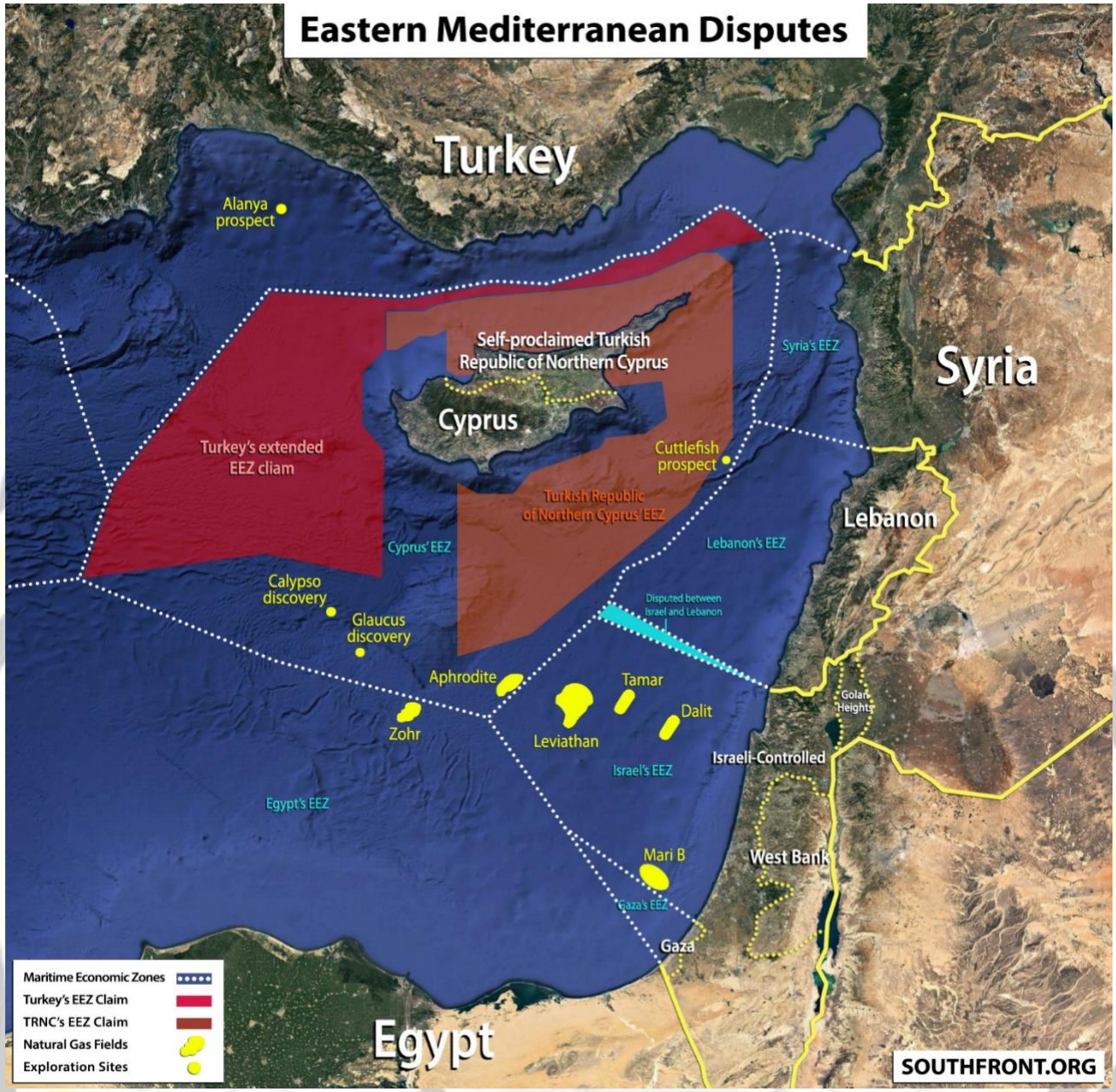
2.5 DOES TENSION TURN INTO MILITARY CONFLICT?

The Eastern Mediterranean is a region where military activity has increased in the recent period. Due to the Syrian issue, countries such as the Russian Federation, the United States, Great Britain and France have an important naval force in this region.

Turkey and Greece are in a major military activity in the region. Concern that limiting the presence in the region in Turkey came up with the blue-2019 exercises his homeland in recent years. It is observed that Greece and Cyprus have increased their exercises in the region.

The latest military tension in the region was the result of Turkish warships blocking ENI's SAIPEM2000 drill ship, which was trying to arrive in early 2018, off Cyprus. Turkey, Greece a frigate conducting research in the October 2018 Barbaros Hayrettin Paşa open Morphou Cyprus announced that harassed the seismic research vessel.

Although it is a risk, the parties will not risk a conflict in which they will ultimately harm their own interests.



2.6 WHAT IS THE MAIN POLICY OF THE PARTIES?

Cyprus is seeking to turn its natural gas resources into economic wealth in the last 10 years. Stating that the Turkish side will benefit from the income to be obtained and a fund will be created for this, the Cyprus government aims to ease the pressure from the international community, especially the UN.

Turkey is in a difficult situation in the international plan to reduce the Cypriot government targets, in line with this policy, the end of the negotiationprocess under UN supervision to spread unless predicts a deficit. If Turkey continues to move against the policy he saw as Cyprus unilaterally.

He just tries to negate the eastern Mediterranean policy will tighten the Gulf of Antalya Turkey side, both he and mobilizes their resources to protect the rights of Turkish Cypriots.

In Greece, which went to early elections on July 7, power changed, the radical left coalition (SYRIZA) finished second and the New Democracy Party came to power on its own. Nikos Dendias (Member of the Greek Parliament) will head the country's new Foreign Minister, in his first week, "Turkey in the Eastern Mediterranean stop being naughty child should be a serious player," he said.

Turkey's Foreign Ministry said, "We find it strange to Dendias statement. 'Spoiled child of Europe' title essentially belongs to Greece," he said and added:

"The naughty child of Europe is the Greek Cypriot Administration, which is a member of the European Union in contradiction with international law and has been dragging the Eastern Mediterranean to the instability with Greece for years."

2.7 QUESTIONS TO BE ADDRESSED

1) Which steps should NATO take to resolve this issue in a peaceful manner?

2) What policy should the parties follow in order to transform this conflict area into a cooperation area and to provide a fair and permanent solutions?

3) How should the Greeks giving the natural gas exploration rights to the big Western States (like Exxonmobil, ENI, TOTAL) evaluated with the NATO? What policies should be established about this issue in regards of policies?

4) What should be the terms of use for natural gas exploration in controversial areas?

5) Is Turkey should take into account the sovereign rights of Cyprus? Should Turkey go to compromise?

3.INTRODUCTION TO THE SECOND AGENDA: CYBERSPACE IN THE CONTEXT OF INTERNATIONAL SECURITY

What distinguishes today's society from the industrial society of yesterday is that different segments of today's society are connected on a global scale through networks (transport, communication, internet). The concept of Global Village Mc, which McLuhan predicted and started to use in the 1960s, is a fact that has been realized to a great extent for a significant part of the world through these networks. Therefore, one of the most important parts of today's social structure is the so-called cyber space. With the increasing use and widespread use of this field, some new threats and weaknesses arising from this field are emerging on a global scale. There are two important developments against these threats and security weaknesses. Firstly, this area is increasingly being secured. The second is that this area is increasingly being addressed by military organizations as a result of this securitization.

Today, military authorities are at the forefront of the ranking of cyber security-related institutions in the US in terms of responsibility. The establishment of a cyber command (USCYBERCOM) in 2010 after the command of air, land, sea and space in the USA and the appointment of a general level at the head of this unit. is one of the clear indications that these elements can be used in this field (O'Connell 2012). In 2008, following Estonia's cyber-attack, Estonia's initiatives led to the opening of NATO's cyber security center of expertise (NATO CCD COE) in Tallinn, the capital of this country. It is also important to illustrate the extent to which this issue has been secured / not militarized.

A direct result of these two developments is that the security dilemma, which is one of the classical concepts of International Relations, that is, the measures taken by one side for its own security, have an unsecuring effect on the other parties and push them to take counter measures, and this is a rapidly proven concept in the field. (Valeriano and Maness 2012). In this context, up to thirty countries, including major powers such as Russia, China and India, are now striving to establish US-like cyber security units and to increase their military capacity in this field, with each country noting that this country is not lagging behind from other countries or countries. Makes financial and military strategic investments in the field.

As a result of all these developments, the concepts of cyber security and cyber war are among the most interesting topics in the field. When the studies on this subject in the field are examined carefully, it will be seen that basically two types of opposing views prevail. The first one considers cyber security as a real and serious national security issue and it is suggested that the

phenomenon that we call cyber war will become a reality with the development of cyber attack tools such as aircraft, missiles or nuclear technology and the development of an effective attack and defense instrument (over time). Alexander 2008; Arquilla and Ronfeldt 1993; Arquilla 2012). In contrast to this, the claim that cyber security is over-exaggerated and that, compared to conventional attacks, cyber attacks will never have a very destructive effect contrary to expectations, and in this context, as a concept, cyber war cannot be defined as a war within the framework of classical war and conflict theories. (Ranum 2003; Libicki 2007; Schneier 2010). As can be seen, both concepts- cyber security and cyber warfare- are a positive and negative opposing view.

3.1 CYBER SECURITY AS A COMPONENT OF INTERNATIONAL SECURITY

Cyber Space has brought many risks, positive and negative situations like all other cases. This has led to the emergence of a new field such as Cyber Security, which has further expanded the security dimension. The concept of cyber space is a very new field by definition. Therefore, its place in the dictionary of social sciences is still in the development stage.

Technical terminology as technological parameters expand It is formed. However, there is no consensus ontology on all aspects of cyber space yet. Has become a new and very important area. Organizations and supra-organizational structures, rather than states, approach the issue very carefully. Organizations such as NATO for collective purposes approached the issue from a wider and different perspective and emphasized cooperation. In fact, NATO has started to see Cyber Attacks in Cyber Space as a security issue and has identified it as a

priority risk threat. Cyber Security started to emerge in such a significant way it has laid the groundwork for new transformations. With the emergence of cyber space, the realization of the threats posed by the security threats that may occur in this area has caused the studies to increase in this field. The studies were first shaped around security. And the understanding of security in the classical sense in International Relations has begun to change. It is seen that the classical perception of security has begun to give way to Cyber Security as a new form of security understanding. In order to talk about the phenomenon of cyber security, it is necessary to mention three basic areas. These are: access control, authentication and authorization. The coexistence of these three situations clearly demonstrates the situation that the concept wants to indicate.

3.2 SECURITY IN INTERNATIONAL RELATIONS

National Security Concept America after the Second World War The National Security Act (18 October 1947) issued by the congress under the President of the United States-USA- Herry S. Truman. Has reached an important position (Central Intelligence Agency: 2017). The concept is not a definition, but rather the limits of the policies to be implemented. According to Brauch (German political scientist) : National Security was the main criticism of military armament during the two major world wars and in the post-war years. It was used to justify an important change in mentality that extended to militarization. International security, on the other hand, is associated with the security of the state with the security of humanity or with the security of individual or minorities within or within the borders of the state. Securing the state is seen as the best way to protect other reference objects. Therefore, 'national security, as many observers have pointed out, is more appropriately referred to as 'state security'. Security in General Considered in all historical processes, the main subject of the study is the state and it can be defined as taking precautions against the threats against the states themselves.

3.3 CYBERSPACE AND RELATED CONCEPTS IN TERMS OF INTERNATIONAL RELATIONS

WHAT IS CYBERSPACE?

Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large

computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

CYBER POLICIES

The cyber space becomes valid in all areas of life; in this field It shows that various policies should also be developed. The issue of ensuring information and network security in the world, which has become digital and open to cyber space, from defense to health services, military and diplomatic intelligence to transportation, is vital for both individuals and governments.

With the spread of the Internet, many institutions and states exposed to directional attacks; billions of economic losses, service delivery practices are regressed or their knowledge is leaked. When all these are taken into consideration, it reveals that policies regarding cyber space are needed and these policies should be handled in a way that regulates national and international cooperation. The steps to be taken during the stage of cyber policies can be summarized as follows;

- Creating a strategy document for cyber security
- Creating cyber security rules
- To raise awareness about cyber security at national and international level and to create an effective culture
- Creating cyber infrastructures to maximize personal and corporate security
- To create joint mobility, to develop joint projects and collaborations with international and transnational structures such as the EU, NATO and the United Nations.
- Strengthening cyber security policy development studies with R&D policies
- To increase privacy and security by developing national technologies and software.
- To produce coordinated policies with universities and non-governmental organizations and to diversify the process.
- To reduce the lack of human resources at these points by increasing the number of experts in the field of cyber security.
- Establish independent audit mechanisms to oversee cyber security policies

- To create legal regulations.

CYBER ATTACKS / THREATS

Any cyber attack that breaches security against any of the personal and corporate data in the cyber space is defined as cyber threat. Cyber threats include viruses, trojans, phishing on social media, and all attempts to violate personal and corporate data.

Important in the cyber space between threats and classic threats there are differences. The basis of these differences is undoubtedly the opportunities and criteria of predicting threats in advance. Because cyber threats are occurring very rapidly today, as they are carried out over highly accelerated internet networks. One of the differences is in terms of the costs incurred and caused. Even inexpensive instruments can be effective to attack in a cyber environment, while these instruments can cause very high costs for the attacker.

CYBER WARS

Cyber warfare is called as a result of systematic exposure to material and moral damage, to infiltrate the infrastructure systems of the rival state / institution, to render it inoperable, to create public opinion against the rival state, to create effective propaganda.

One of the most important criteria in describing cyber attacks as war is that it occurs between at least two states. On the other hand, doing this systematically takes it beyond cyber attack.

CYBER POWER

Cyber power; ability to use this environment in cyberspace / space, with cyber tools, to gain gains by dominating cyber space, and to influence other actors of cyber space with these gains and cyber tools.

This definition made in the name of cyber power; Parameters such as producing effective cyber policies, cyber actions and operations, preventing cyber threats, identifying and tracking the sources of attack threats, having the advantage of being affected but not affected while doing all this can also be expanded by adding parameters. On the other hand, cyber power; There are also opinions that define the ability to do something strategically effective in cyberspace.

CYBER DIPLOMACY

Cyber diplomacy, also called e-diplomacy, digital diplomacy, online diplomacy; Regardless of its name, it emerges as a new form of diplomacy in the information age. Despite its semantic nuances; cyber diplomacy differs from traditional diplomacy in three ways. These; more information, more interaction and more transparency.

Cyber diplomacy in general; It is defined as an aid to international diplomatic activities using the internet and new technological communication tools.

CYBER SECURITY

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users, or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

3.4 CYBER SECURITY AND INTERNATIONAL RELATIONS

To ensure the protection of personal privacy in Cyber Space The importance of dynamics such as technological infrastructure, systems and users comes to the fore. It is very important to create systems that prioritize the safety of users by experts in the field. Information equipment must be complete in terms of the operability of the systems and the users not to make various mistakes.

Cyber Security Situations Occurring in the International System

2007 Cyber Attack on Estonia

There was a constant conflict between Russia and Estonia after the dissolution of the Soviet Union. The last point of the dispute was that relations escalated after Estonia lifted the former Soviet Soldier Monument in the center of Tallinn on April 26, 2007. The night has passed into the history scene as Bronze Night. In this process, Estonia, which also included the intense Russian minority, was subjected to three weeks of intense cyber attacks.

In the country where Europe's strongest cable society and e-government application are at the highest level, cyber attacks have brought life to a halt. The target point of the attacks; There were the Estonian Presidency and Parliament, Political parties, all government ministries,

the country's three major news organizations, the largest bank and companies specialized in communications.

After the attack, Estonian Defense Minister Jaak Aaviksoo said in a statement; It states that NATO did not define cyber attacks as an open military operation, and that it came from the provisions of Article 5 of the North Atlantic Treaty or that the collective defense mechanisms of another system would not be extended automatically to the country under attack. Likewise, NATO's defense minister has also been sent in the statement, we cannot define Cyber attack as an open military action at the moment. However, there is a statement that this issue should be resolved in the near future (The Guardian, 2007).

The important point here is that if this attack was defined as war, NATO would have to collectively face Russia. Likewise, the Estonian defense minister initially stated that he considered it a war, but no such feedback from NATO was ever provided. Therefore, the explanations made were that it would be accepted and investigated more moderately as an attack. Likewise, Kremlin spokesman Dimitri Peskov stated that the allegations were unrealistic and explained that Russia was not responsible (BBC Turkish, 2007).

However, the researches of the experts show that the attacks are carried out with the method known as DDos (Distributed Denial of Service). It was revealed that many computers were seized and made by turning them into zombies. It is determined that the main computers where zombie computers are used are in Russia and written in the program in Kril alphabet (Clarke, Kanke, 2011: 15).

The Estonian attack raised an important question in the International arena. It brought up how the state faced with such a situation would react or create a defense mechanism against the attack. Here, the point where the relative strengths of the states depend on the importance of the responses is noteworthy. In the incident that occurred in 2007, Estonia's direct accusation of the Russian Government after Russia started its attacks caused the two states to face each other. Estonia wanted to start collective self-defense by wanting to take advantage of NATO membership. However, NATO refrained from blaming Russia for an armed attack. The Estonian Defense Minister compared the disappointment of the service activity with the terrorist activities directly. He continued to state that the attack came from computers within the Russian cyber space. The incident was expressed as an attack, not as a war in NATO or EU. The absence of war here was expressed as substantial material damage or no harm to people. Aaviksoo acknowledged that neither the EU nor NATO could be described as cyber warfare nor could it

identify the rights of member states and what the EU and NATO had to bear in the event of such attacks. It is clearly stated that cyber attacks are difficult to define as a clear military action. In short, it was stated that Article 5 of NATO does not mean that it would be implemented automatically (Farwell, Rohozinski, 2011: 32).

Statements by NATO and the EU show that in the face of such attacks, states are actually alone because of the anarchic environment created by the Cyber Space. It has been clearly understood how nearly 60 percent of its people provide most of their daily needs from the internet, and about 96 percent of the banking transactions in the country, such as Estonia, which takes place over the internet, would be compromised by such attacks (Yener, 2015).

2008 Cyber Attack on Georgia

It is seen that many ethnic and intra-state problems have been experienced for many years in the territory of the USSR, which dispersed with the end of the Cold War. Another one of these is the South Ossetia problem, which became de facto independently in Georgia but is still considered to be affiliated to Georgia in the international arena. Although South Ossetia was affiliated with Georgia, it received considerable support from Russia in general. By August 2008, some separatist movements were observed in the South Ossetia region. The Georgian government, on the other hand, started to organize a military operation in the Ossetia region in order to stop these separatist movements. After this operation, Russia went to Ossetia. and supported Georgia, it carried out both military and cyber attacks.

There are some points that make the war between Georgia and Russia important and distinguish it from other classical meaning wars. First of all, Russia carried out cyber attacks to support its military operations. It attacked the government sites and many commercial websites and brought the war to virtual realm (The Sydney Morning Herald, 2008). In fact, these attacks started before the military attacks started. Just as long as 20 weeks before the war broke out, Russia seized thousands of computers in many countries and launched attacks against Georgia. During this period, it was clearly seen that he was slowly deploying troops on the borders of Ahbazya and Ossetia (Newsweek, 2008). Since the beginning, the Georgian government has accused Russia. Instead of rejecting this situation, the Russian side has brought the accusations to the point of accepting the accusations, "There are people trying to do something for their country." The attacks caused the internet access to cease for days in the country. Even power cuts were experienced and the country was tried to be disconnected from the outside world (The New York Times, 2008).

The results of the detailed research carried out one year after the attacks have also confirmed this explanation. It clearly demonstrated that the attacks were organized in Russia by the youth movement against anti-Russian and anti-Russian activists (The Register, 23.03.2009). In addition to this, Sanka Petersburg-based Russian Business Network (RBN) from several computers on the internet institutions of Turkey and Russia have understood that the attacks carried out by passing the hand (Deutsche Welle, 2008).

The importance of attacks in the international system and discipline; It is the attacks that started in the cyber space for the first time, turning into an armed conflict and taking the form of war. It is seen that this situation was not experienced explicitly in many attacks. However, the Russia-Georgia conflict represents the first major cyber attacks accompanying the armed conflict (Nye, 2008).

Russia was a significantly strong country in the field of cyber attacks. These attacks can be perceived as a clear message to the West and the world. The Russian Government, which proved that cyber attacks can turn into war, also wanted to create a deterrence effect. He made an effort to prove that he was a great power again after the Cold War and emphasized that he had a say in his region. An example of this is the fact that after the US decided to establish a military base in Kyrgyzstan in 2009, the country's 4 major service providers remained under intense attacks (TimeTurk, 2013). Taken together, the Georgia attack has shown that cyber attacks are a potential force for deterrence (Goodman, 2010: 104).

3.5 QUESTIONS TO BE ADDRESSED

1) How can you prevent governments cyber attacks against each other?

2) How should the policies of cyberspace be determined?

3) How should cyberspace be in the international relations?

4) Which path should be followed in case of violation of cyber security policies?

5) What should be the attitude and policy of NATO in a possible cyber war between NATO members?

4. REFERENCES

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190218_190218-WhatIsNATO_en.pdf

https://en.wikipedia.org/wiki/2018_Cyprus_gas_dispute

https://www.bbc.com/turkce/haberler-dunya-48225246

https://kureselcalismalar.com/uluslararasi-iliskilerde-siber-uzay-siber-guvenlik-ve-siber-savas-gecmis-gunumuz-ve-gelecek/

http://afyonluoglu.org/PublicWebFiles/Reports-TR/Akademi/2018-KAmil%20Tarhan-Uluslararas%C4%B1%20g%C3%BCvenli%C4%9Fin%20bir%20bile%C5%9Feni%20olarak%20siber%20g%C3%BCvenlik.pdf