# INFORMATION WARFARE CAPABILITY OF A NON-STATE ARMED ACTOR:

# A CASE STUDY OF THE ISLAMIC STATE OF IRAQ AND SYRIA

**ELİF BUDAK**

**JANUARY 2022**

# INFORMATION WARFARE CAPABILITY OF A NON-STATE ARMED ACTOR:

# A CASE STUDY OF THE ISLAMIC STATE OF IRAQ AND SYRIA

**A THESIS SUBMITTED TO THE**

**GRADUATE SCHOOL**

**OF**

**BAHCESEHIR UNIVERSITY**

**BY**

**ELİF BUDAK**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR**

**THE DEGREE OF MASTER OF GLOBAL AFFAIRS**

**IN THE DEPARTMENT OF GLOBAL AFFAIRS**

**JANUARY 2022**

**T.C.**
**BAHCESEHIR UNIVERSITY**
**GRADUATE SCHOOL**

…/…/….

MASTER THESIS APPROVAL FORM

| | |
|---|---|
| **Program Name:** | GLOBAL AFFAIRS |
| **Student's Name and** | ELİF BUDAK |
| **Name Of The Thesis:** | INFORMATION WARFARE CAPABILITY OF A NON-STATE ARMED ACTOR: A CASE STUDY OF THE ISLAMIC STATE OF IRAQ AND SYRIA |
| **Thesis Defence Date:** | 26.01.2022 |

This thesis has been approved by the Graduate School which has fulfilled the necessary conditions as Master thesis.

**Prof. Dr. Ahmet ÖNCÜ**
**Institute Director**

This thesis was read by us, quality and content as a Master's thesis has been seen and accepted as sufficient.

| | **Title/Name** | **Signature** |
|---|---|---|
| **Thesis Advisor's** | Asst. Prof. Zekeriya TÜZEN | |
| **Member's** | Assoc. Prof. Esra ALBAYRAKOĞLU | |
| **Member's** | Asst. Prof. Ahmet İlkay CEYHAN | |

I hereby declare that all information in this document has been obtained and presentedin accordance with academic rules and ethical conduct. I also declare that, as requiredby these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname : Elif BUDAK

Signature :

## ABSTRACT

INFORMATION WARFARE CAPABILITY OF A NON-STATE ARMED ACTOR:
A CASE STUDY OF THE ISLAMIC STATE OF IRAQ AND SYRIA

Elif BUDAK

Global Affairs Master Program

Thesis Supervisor: Asst. Prof. Zekeriya TÜZEN

January 2022, 94 pages

This study aims to illustrate the information warfare capability of a non-state armed actor over a case. The reason for the selection of the subject is the growing influence of non-state armed actors on asymmetric and hybrid warfare pitches. In this manner, the study predicated on mainly five types of information warfare such as command and control, psychological, cyber, economic, and electronic warfare and inserted them into the Islamic State of Iraq and Syria, which it chose as a case. The methodology of the study is the qualitative analysis being predicated on a case study.

The capacity of the Islamic State of Iraq and Syria to conduct simultaneous operations in Iraq and Syria, the ability to attract the attention of the whole world by exploiting both traditional and modern tools of psychological warfare and, to a lesser extent, its utilization from cyberspace which is a new battlefield after land, air, and sea revealed that the Islamic State of Iraq and Syria had information warfare capability. However, the group was not integrated into the legitimate economic system to wage economic warfare and did not have the adequate electronic capacity to conduct electronic warfare. Therefore, the information warfare capability of the Islamic State of Iraq and Syria was not at a level to have superiority over states or compete with them.



**Keywords:** Non-State Armed Actor, the Islamic State of Iraq and Syria, Information Warfare

# ÖZET


DEVLET DIŞI SİLAHLI BİR AKTÖRÜN BİLGİ HARBİ KABİLİYETİ:
IRAK VE SURİYE İSLAM DEVLETİ ÖRNEĞİ

Elif BUDAK

Küresel İlişkiler Yüksek Lisans Programı

Tez Danışmanı: Dr. Öğr. Üyesi Zekeriya TÜZEN

Ocak 2022, 94 sayfa

Bu çalışma devlet dışı silahlı bir aktörün bilgi harbi kabiliyetini bir vaka üzerinden göstermeyi amaçlamaktadır. Konunun seçilmesinin nedeni devlet dışı silahlı aktörlerin asimetrik ve hibrit harp sahalarında artan etkinliğidir. Bu minvalde, çalışma kumanda ve kontrol, psikolojik, siber, ekonomik ve elektronik olmak üzere başlıca beş bilgi harbi çeşidini esas almış ve bunları vaka örneği olarak seçilen Irak ve Suriye İslam Devleti'nin bilgi harbine yerleştirmiştir. Çalışmanın metodolojisi, bir vaka çalışmasına dayanan nitel analizdir.

Irak ve Suriye İslam Devletinin Irak ve Suriye'de eş zamanlı operasyonlar yürütme kapasitesi hem geleneksel hem de modern psikolojik harp araçlarını kullanma yeteneği ve daha az ölçüde de olsa, kara, hava ve denizden sonra yeni bir savaş sahası haline gelen siber uzaydan yararlanması Irak ve Suriye İslam Devleti'nin bilgi harbi kabiliyeti olduğunu ortaya çıkarmıştır. Ancak, grup hem ekonomik harp yönetecek meşru bir ekonomik sisteme dahil değildi hem de elektronik savaş yürütebilecek düzeyde yeterli elektronik araca sahip değildi. Bundan dolayı, Irak ve Suriye İslam Devleti'nin bilgi savaşı kabiliyetinin, devletler üzerinde üstünlük sağlayacak ya da onlarla rekabet edebilecek düzeyde olmadığı sonucuna varılmıştır.



**Anahtar kelimeler:** Devlet Dışı Silahlı Aktör, Irak ve Suriye İslam Devleti, Bilgi Harbi

**ACKNOWLEDGEMENTS**

I wish to express my deepest gratitude to my thesis supervisor Asst. Prof. Zekeriya TÜZEN for his guidance, advice, criticism, encouragement, and insight throughout the research.

I would also like to thank my family as a whole for their continuous support and understanding when undertaking my research and writing my thesis.

## TABLE OF CONTENTS

ETHICAL CONDUCT ..... iii

ABSTRACT ..... iv

ÖZET ..... v

ACKNOWLEDGEMENTS ..... vi

TABLE OF CONTENTS ..... vii

LIST OF FIGURES ..... x

LIST OF ABBREVIATIONS ..... xi

Chapter 1: Introduction ..... 1

Chapter 2: Information Warfare: The Definition, History, And Types Of The Concept Of Information Warfare ..... 7

2.1 Definition of Information Warfare ..... 7

2.2 Historical Background ..... 9

2.2.1 Information Operations ..... 10

2.2.2 Hybrid Warfare ..... 11

2.2.3 Asymmetrical Warfare ..... 14

2.3 Types of Information Warfare ..... 15

2.3.1 Command and Control Warfare ..... 16

2.3.2 Psychological Warfare ..... 17

2.3.3 Cyber-Warfare ..... 23

2.3.4 Economic Warfare ..... 25

2.3.5 Electronic Warfare ..... 28

Chapter 3: The Involvement Of The Islamic State Of Iraq And Syria In Information Warfare ..... 31

3.1 The Islamic State of Iraq and Syria as A Non-State Actor ..... 31

3.1.1 The Overview of ISIS ..... 33

3.1.2 The Reasons for The Rise and Spread of ISIS ..... 35

3.1.3 The Global Coalition to Defeat ISIS ..... 37

3.2 Placing The Information Warfare in Warfare of ISIS ..... 38

3.2.1 Command and Control Warfare of ISIS ..... 38

3.2.1.1 Knowledge and experience ..... 38

3.2.1.2 Operational picture and information flow ……..40
3.2.1.3 Confidence/Trust ……43
3.2.1.4 Situation awareness ……43
3.2.1.5 Objectives ……...44
3.2.1.6 Feedback ……44
3.2.1.7 Flexibility ……45
3.2.1.8 Decision making ……46
3.2.2 Psychological Warfare of ISIS ……..47
3.2.2.1 The media strategy of ISIS ……48
3.2.2.1.1 Traditional media ……48
3.2.2.1.2 Social media ……52
3.2.2.2 Image war of ISIS ……54
3.2.2.3 Strategic communication and ISIS ……55
3.2.3 Cyberwarfare of ISIS ……56
3.2.3.1 Cyber strategy of ISIS ……57
3.2.3.1.1 Recruitment strategy ……58
3.2.3.1.2 Intimidation strategy ……59
3.2.3.1.3 Provocation strategy ……60
3.2.3.1.4 Outbidding strategy ……61
3.2.3.2 Cyber Caliphate ……62
3.2.3.3 Dynamics of ISIS'S cyberwarfare ……63
3.2.4. Economic warfare of ISIS ……64
3.2.4.1 Revenues ……65
3.2.4.1.1 Taxes, Fees, and Extortion ……66
3.2.4.1.2 Looting, Confiscations ……67
3.2.4.1.3 Natural Resources ……67
3.2.4.1.4 Kidnapping Ransoms ……68
3.2.4.1.5 Other Sources of Income ……68
3.2.4.2 Dynamics of Economy of ISIS ……...69
3.2.5. Electronic Warfare of ISIS ……...71

Chapter 4: The Information Warfare Capability Of Isis: The Answering Of The Research Sub-Questions ……75

4.1 Information Warfare Capability of ISIS ……...75
4.1.1 Command and Control Capability of ISIS ……75
4.1.2 Psychological Warfare Capability of ISIS ……78
4.1.3 Cyberwarfare Capability of ISIS…… 80
4.1.4 Economic Warfare Capability of ISIS ……...…81
4.1.5 Electronic Warfare Capability of ISIS ……..……..83

4.2 The Evaluation of The Information Warfare Capability of ISIS …..….84

Chapter 5: Conclusion ……90

REFERENCES .....95

## LIST OF FIGURES

Figure 1 A Digital Rendering of Haji Bakr's Islamic State Organigram..... 42
Figure 2 Summary of the Organization's Media Products..... 49
Figure 3 ISIS Revenue, Source ICSR.. ..... 66

## LIST OF ABBREVIATIONS

| | |
|---|---|
| CBRN | Chemical, Biological, Radiological, and Nuclear |
| CENTCOM | United States Central Command |
| CNO | Computer Network Operations |
| ISIS | Islamic State of Iraq and Syria |
| MILDEC | Military Deception |
| NNSA | Non-State Armed Actor |
| OODA | Observe, Orient, Decide, Act |
| OPSEC | Operational Security |
| UAV | Unmanned Aerial Vehicle |
| UCC | United Cyber Caliphate |
| USAF | United States Air Force |
| USSR | Union of Soviet Socialist Republics |
| WMD | Weapon of Mass Destruction |

# 1. INTRODUCTION

Owing to the development and increase of technology, the flow of information has gained momentum in numerous fields. Together with globalization and the facilitation of access to mass communication, the accessibility of information has never become more accessible. However, these opportunities to easily access information by non-state armed actors (NSAA)s have enabled these groups to fulfill their actions, which have gained organized and multifaceted aspects, to the detriment of local, regional and global entities. So, this work attempts to scrutinize and measure whether NSAAs have the ability to exploit the concept of information warfare and have relative superiority over states in conducting information warfare.

Since ancient times, every entity, such as individuals, local authorities, states, organizations, has seen security as a necessity in order to protect themselves, continue their existence, and prosper. In order to provide security, entities have sought to obtain information that required them to have an advantage over others. The desire to have strategic information that would be a trump against rivals resulted in an information war to come out among competitors. In this manner, although information warfare as a term was not used until 1976[1], invisible information wars existed among individuals, states, and organizations. They have gradually improved new ways and methods of attaining information to gain an advantage over their adversaries. Thanks to ever-growing and developing technology, as a new term, "information technology" emerged as of the 1950s. The utilization of information technologies such as computer systems, communication systems, every kind of software and hardware equipment has accelerated the emergence of new ways and methods of attaining information. Therefore, the concept of information warfare has stepped into a new dimension where exploited modern practices and techniques alongside conventional ones. After this new stage, information warfare became more complex, sophisticated and gained an asymmetric form consisting of psychological, informatics, military, and economic aspects. As a result, many entities, including mass communication, electronic

[1] The term was used by Thomas P. Rona as information war in its work dated July 1, 1976 and called "Weapons systems and information war."

reconnaissance, surveillance tools, financial system instruments, military weapons and ammunition, and rocket and missile systems, got involved in the information warfare issue among states, organizations, terrorist groups, and individuals.

The aim of the thesis is to illustrate the information warfare capability of an NSAA over a case and offer a perspective regarding how NSAAs use it. It also includes attempts to analyze their relative capability over the states. This study will present a different perspective regarding the issue of information warfare by referring to an NSAA. Although various studies pertaining to information warfare currently exist on this subject, these studies generally focus on the detailed sub-headings of information warfare and have been viewed in terms of the technical aspects in various articles. This study differs from existing studies relating to information warfare as it presents a new framework that focuses on the usage of information warfare by an NSAA. First, this study outlines the concept of information warfare by discussing its various types and conceptually addresses the topic of NSAA. After the introduction of some conceptual frameworks related to information warfare and NSAAs, the study will then examine the issue over a case study. In doing so, the study will focus on the capability of an NSAA in conducting information warfare and strive to find out whether an NSAA can have the information warfare capability.

Following World War II, some states gained independence, giving rise to emerging local militias and armed groups in those countries. These armed groups have been prominently seen since the 1990s after the collapse of the Union of Soviet Socialist Republics (USSR). Armed groups are especially visible in countries within the Middle East, Asia, and Africa, where robust regimes and state authority do not exist. As a result of violence, conflict, and civil wars in these countries, NSAAs have been trying to take over these regions by benefiting from weak regimes and authorities. In time, these groups have achieved access to a large number of weapons, extensive sources of finance, knowledge, experience, and an enormous opportunity and ability as such. NSAAs, which execute terrorist activities, illegal actions, and various crimes, have almost reached such a position that they have the ability to compete with states in regards to both in terms of traditional and unconventional ways. In recent years, their ability to attain economic resources, operational capability, organizational actions, and the ability to achieve their goals to a certain extent presents some

examples that provide us the opportunity to consider how much power these groups have gained.

The importance of the study is to tackle an NSAA in terms of information warfare, which involves various fields ranging from social, economic, political, to military, has significance as no such research comprising information warfare and NSAAs have directly been found in the literature. The study purposes of presenting a new perspective for the information warfare concept by measuring the capability of an NSAA in the information warfare domain. At the same time, it aims to contribute to the academic literature by measuring the ability of NSAA on this issue.

The methodology of the study is the qualitative analysis being predicated on a case study. A case study is a research strategy grounded in an experimental example that tries to inquire and explain a phenomenon within a practical context. Based on the collected text and image data, the qualitative method involves discussing the sample for the study and expands on the data analysis steps and the methods used for presenting the data, interpreting it, validating it, and indicating the potential outcomes of the study (Creswell, 2014, pp. 183-185). Qualitative research is a method in which the researcher attempts to reach a conclusion regarding the research question resulting from interpreting the data obtained by analyzing and synthesizing different data sources such as books, newspapers, electronic resources, and articles. In this sense, the study looked into and handled books and articles related to the concept of information warfare, the Islamic State of Iraq and Syria (ISIS) chosen as the case for this study, and the way of ISIS's information warfare that would constitute the theoretical, practical, and empirical framework for the study.

Further, the study also benefitted from various electronic resources such as web pages/sites, newspapers, and released reports to exemplify incidents, happenings, and statistics. Qualitative analysis is preferred because the subject of this study is suitable for the nature of qualitative research, which strives to analyze, interpret, and understand concepts, thoughts, cases, and experiences. In this context, this study will examine an NSAA capability on a case from the point of view of information warfare, and for this purpose, it will benefit from the documents collected, interpret the findings based on qualitative analysis, and then conclude by answering the research questions.

The main research question of the study is, does an NSAA have information warfare capability? If it has, does an NSAA have any superiority over states in terms of information warfare capability? The capability of NSAAs to access information and use information systems has developed to such a position that it brought to mind the question of whether NSAA can compete with states in terms of information warfare. Within this direction, the study will research the information warfare capability of an NSAA and try to answer these questions.

Studies on the concept of information warfare that can find a place in various academic disciplines relevant to social studies from political science, psychology, economics, to sociology were substantially handled in terms of the military in literature. The concept of information warfare by its nature is also so compatible with the international relations field, as will be seen in this study. The thesis aims to illustrate the information warfare capability of an NSAA, and in this manner, it handled ISIS as a case. However, the studies on information warfare based on ISIS in the field of international relations mostly centered on psychological warfare and, to a lesser degree, cyber warfare. In this regard, the study faced a shortage of resources respecting other types of information warfare. The challenges of writing this research are relevant to the topic of information warfare that contains a complex and extensive area and limited studies on this subject.

The subject of the study is the information warfare capability of an NSAA, a case study of ISIS. The reason for determining this subject is the emergence of a new world order with the constantly evolving technology and, as a result of globalization, the disappearance of the borders between the states and the inclusion of new actors in the global system as a variable and ultimately, the possibility that asymmetric wars among these actors will shape the future. As a case, ISIS followed quite sophisticated and advanced modus operandi compared with other armed actors. It had established a hierarchical structure, pretended like a state, and amalgamated conventional and non-conventional methods while performing its objectives. In order to measure the capability of ISIS in terms of information warfare, the years of 2014, 2015, and 2016, when the terrorist group had reached its peak and, the world had been astonished and began to react to the group’s actions, were taken as the basis in the study.

The study attempts to answer the research question by addressing the following five sub-questions: 1- Can the command-and-control ability of an NSAA compete with states? 2- Does an NSAA successfully use traditional and modern methods while conducting psychological operations? 3- Has an NSAA become a threat to states in terms of cyber warfare? 4- Could an NSAA engage in economic warfare with the states? 5- Does an NSAA have sufficient electronic warfare capacity in terms of the electromagnetic spectrum to a certain extent?

This thesis is composed of five chapters, including the introduction and conclusion chapters. The introduction chapter subsumes a general framework related to the concept of information warfare and the Islamic State as a selected NSAA case. It clarifies the importance and purpose of the study and determines the research questions alongside a couple of sub-questions.

The second chapter (Information Warfare: the definition, history, and types of the concept of information warfare) of this study offers a conceptual framework pertinent to information warfare. After a short discussion of the evolution of information warfare, this chapter provides the reader with brief but comprehensive definitions of information warfare and related terms. This chapter also analyzes the various types of information warfare that would constitute a basis for the research questions and sub-questions due to being the center of the subject.

The third chapter (The involvement of the Islamic State of Iraq and Syria in Information Warfare) touches upon a brief history of non-state armed actors and presents an overview of ISIS as an NSAA regarding its ideology, purpose, strategy, leadership, recruitment, and why it arose and spread. Furthermore, it tried to integrate the way of ISIS's usage of information into the main five types of information warfare; command and control warfare, psychological warfare, cyber warfare, economic warfare, and electronic warfare. For this reason, it firstly analyzes ISIS's command and control warfare by examining nine perquisites of command-and-control ability in terms of ISIS. It defines every prerequisite of command-and-control warfare by inserting these prerequisites into the way of ISIS's adaptation and tries to measure whether it has adequate command-and-control ability capacity. Secondly, the chapter handles the issue of psychological warfare by explaining ISIS's media strategy, which

the group blended with traditional and social media. It aims to explain how the group used its media strategy as a propaganda tool while waging its psychological warfare. Thirdly, it inquires whether ISIS had a considerable capability to handle cyberspace and perform sophisticated cyber-attacks that culminate in its leakage to computers and destruct state infrastructures in terms of cyber warfare. Fourthly, it explains the economy of ISIS by illustrating its revenue and expenditure items and its volatility against external factors. Finally, the chapter evaluates ISIS's electronic device and weapon capacity based on the electromagnetic spectrum.

The fourth chapter (the Information Warfare capability of ISIS: the answering of the research sub-questions) focuses on the findings captured in the previous chapter. In line with these findings, the chapter independently analyzes each type of ISIS's information warfare by measuring the group's capability on this subject. To that end, the chapter tries to clarify whether the terrorist organization can have the ability to conduct information warfare victoriously.

In the conclusion chapter, the study discussed the results of the research sub-questions and answered the main research question. Ultimately, the study deduced that ISIS had the information warfare capability to a certain extent; however, this extent was not sufficient for it to have superiority over states and compete with them.

# 2. INFORMATION WARFARE: THE DEFINITION, HISTORY, AND TYPES OF THE CONCEPT OF INFORMATION WARFARE

Information is a combination of arranged data that is necessary to eliminate uncertainty or reduce it. Those who have information have provided relative superiority to various individuals, groups, or organizations that do not have the same or equivalent information. Thus, the more the organisms obtain information, the more they have comparative advantages and privileges. This situation has conduced to the tactical and strategic use of information in various fields such as politics, economic, military, and social against rivals or adversaries. Moreover, the technological advancements and the development of information technologies have contributed to the emergence of the concept of information warfare.

The chapter firstly touches upon the definition of information warfare and ascribes it as a strategic warfare that provides a competitive advantage over other elements. Then, after giving brief information about the history of information warfare, it mentions information operations that involve the overall attempts to destroy, corrupt, and exploit information, hybrid warfare that composed of a combination of procedures including conventional and unconventional methods, and asymmetric warfare that rooted in irregular warfare among states and non-state actors that are relatively weak against states. Finally, at the very end, the chapter handles and explains the five types of information warfare that will form a basis for the research question and sub-questions: command and control warfare, psychological warfare, cyber warfare, economic warfare, and electronic warfare.

## 2.1 Definition of Information Warfare

Information warfare as a term was used firstly by Thomas P. Rona in his report "Weapon Systems and Information War" for the Office of the Secretary of Defense Washington DC, July 29, 1976 (Rona, 1976). Martin C. Libicki who is a scholar and professor, offers information warfare by referring to Thomas P. Rona's definition: "The strategic, operational and tactical level competitions across the spectrum of

peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives" (Libicki, 1995, p. 4).

This definition emphasizes that the information warfare concept is not limited by wartime as it also comes into existence in peacetime. It is almost preliminary to war, protection from the war, or a tool provided to reach goals and is a process that consists of observation, orientation, decision-making, and action. In this point, the nature of information warfare overlaps with the OODA Loop (Observe, Orient, Decide, Act) developed by John Boyd, who was a fighter pilot and military strategist (Kopp, Korb, & Brumley, 2012).[2] The OODA Loop is a strategy that individuals and groups in various fields can use in order to achieve their objectives.

Another definition is given by Ronald Fogleman (General, United States Air Force (USAF)) and Sheila E.Widnall (Secretary of the Air Force) is that "Information Warfare: any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions" (Fogleman, Widnall, & United States Air Force, 1997, p. 1).

In the aforementioned definition by Fogleman, the enemy's information and its functions refer to physical tools, control-command systems, and the human mind. As can be understood from this definition, the information warfare concept involves a process of defending information, attacking information, and exploiting information in a variety of ways. In this process, it aims to infiltrate the enemy's information functions in order to destruct and corrupt information systems and, in this way, enable an attempt to deceive and misdirect the enemy.

[2] The OODA loop (Observe, Orient, Decide, Act) model is a method of representing the decision-making and action cycles of an entity. It was originally developed to model the decision-making process of fighter pilots; however, its generality makes it suitable for modelling most decision-making cycles. Boyd's OODA Loop is a four-step cyclic model, which describes the information gathering, decision making and actions of an entity, with earlier behavior providing feedback to the current analysis and decision activities. Brumley, Lachlan, et al. "Cutting Through the Tangled Web: An Information-Theoretic Perspective on Information Warfare." *Air Power Australia Analyses*, vol. IX, no. 2, Oct. 2012, p. 1, http://www.ausairpower.net/APA-2012-02.html.

As a result, it can be deduced from these definitions that the information warfare concept explains strategic warfare to provide a competitive advantage over other elements to defend, attack, and protect by benefiting from information systems and information technologies. Information warfare is a method of war without fighting. As Sun Tzu said, “Every battle is won before it’s ever fought.” There are various types of information warfare, such as command and control warfare, intelligence-based warfare, electronic warfare, cyber warfare, psychological warfare, and economic warfare.

## 2.2 Historical Background

Throughout history, individuals, groups, and states have fought one another for political, economic, and social reasons. History has witnessed these actors in various conflicts aimed at maintaining their existence. Sun Tzu, a renowned Chinese military scholar, philosopher, and general, wrote the oldest and highly disputed war strategies in his famous book “The Art of War.” Sun Tzu put forward the thought that “all warfare is based upon deception.” Even today, his book includes various strategies ranging from laying plans, maneuvering, and considering terrain to intelligence and has been a primary referenced book not only in the military domain but also in other fields. The exploitation of the Egyptian correlation of cats to divinity led to the Persians gaining their victory at Pelusium by painting their shields with the image of cats in The Battle of Pelusium in 525 B.C. (Stephens, 2020, p. 41). This demonstrates how the Persians engaged the knowledge about the sacredness of the cats in its war against Egyptians as a psychological impulse. Additionally, Carl Von Clausewitz, who was a Prussian general and military intellectual, came up with the idea that “war is the continuation of politics by other means” by attributing the relations between war and politics. Clausewitz pointed out the importance of the uncertainty of all information during the war as one of the principal problems in formulating a theory of the war in his book “On War.” He said that “the general unreliability of all information presents a special problem in war,” and he expressed the necessity for clarifying unreliable information.

Based on these examples, it can be said that the importance of information dates back to ancient times, and various parties have used it as both a source and a means of weapon in the course of history. Moreover, parties have exploited strategic information in order to reach their purposes. Although it has never been mentioned until the twentieth century, this illustrated that there was invisible information warfare between parties.

The existence of information warfare is not new; however, it has gained significant prominence following World War II. While conventional methods have been used in the information warfare concept until the twentieth century, with the help of information technologies, unconventional and contemporary techniques, have been added to the information warfare concept. However, information warfare as a term for the first time was used by Thomas P. Rona in his report "Weapon systems and Information war."

Information warfare has two main conceptions. The first is the American concept of information warfare, and the other is the Russian concept of information warfare. The American understanding of information warfare considers it from the point of the military domain rather than other forms of information warfare. Contrary to this, the Russian understanding of information warfare is not limited to war or wartime and is also a type of preparation for war, and Russians mainly exploit psychological warfare, which is one of the types of information warfare.

### 2.2.1 Information Operations

Information operations involve a variety of actions to influence a rivals' information and information system with the purpose to defend, attack, and protect. The broader definition of information operations is "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own" (Homeland Security Digital Library, Joint Publication 3-13: Information Operations, 2014). Contrary to the

conventional war concept, information operations are an unconventional practice of warfare based on information.

Information operations are the overall attempt to destroy, corrupt, and exploit information obtained from various sources in order to bring other elements or enemies under control. Information operations capabilities involve psychological operations (PSYOPS), military deception (MILDEC), operational security (OPSEC), computer network operations (CNO), and electronic warfare (EW).

Daniel T. Kuehl identifies three distinct types of information operations: hardware, software, and wetware (Kopp, Korb, & Brumley, 2012, p. 1). Hardware describes the visible factors of information operations, such as physical appliances of information systems, including communication structures, computers, and satellites. Software describes the invisible elements of information operations, presenting as non-physical appliances of information systems such as the command-and-control instructions of hardware. Wetware represents the human mind in the information environment. This type is the most complex type of information operations, and PSYOPS is highlighted here.

While information warfare attributes a kind of strategy to achieve various objectives in an information environment, both during conflict and peacetime, information operations are actions relevant to information related-capabilities to implement strategies. On the one hand, information warfare is not a new phenomenon; it has been involved in various fields in history and dates back to ancient times. On the other hand, information operations are a new term that dates back a few decades ago and generally is related to the military domain.

### 2.2.2 Hybrid Warfare

Together with increasing and developing information technologies and communication systems, a new perception of war has emerged since the end of the twentieth century. The international system has witnessed a new era in which the conflicts among states have reached the level that individuals, groups, and organizations could be a threat to states. This new face of war, called hybrid warfare,

is a combination of methods, including conventional, unconventional, and non-military tools.

Lawrence Freedman says that hybrid warfare as a "term gained currency after Israel was said to have been surprised and discomfited during the 2006 Lebanon War by the combination of guerrilla and conventional tactics adopted by Hezbollah" (Freedman, 2014, pp. 10-11). Since then, this term has been used to describe conflicts in which conventional and non-conventional methods are contained themselves that have taken place in the various regions of the world.

In today's world, international order witnesses a variety of examples of hybrid warfare in which various methods and ways are used, such as network-centric operations, supporting revolts and terrorism, intimidation of people, information campaigns, covert operations under the image of humanitarian assistance and peace. Frank G. Hoffman explained hybrid wars as follows (Hoffman F. , 2007, p. 14):

> Hybrid Wars can be conducted by both states and a variety of non-state actors. Hybrid Wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder.

In the same way, the world has witnessed several hybrid warfare that have been and are taking place in recent history among different entities; the creation of the Islamic State, the Arab Spring, the crisis in Crimea are examples of ongoing hybrid warfare whose effects have continued.

The Russian view of modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare in order to achieve superiority in troops and weapons control, morally and psychologically depressing the enemy's armed forces personnel and civil population (Bērziņš, 2014, p. 5). Russian intervention in Ukraine is one of the most known cases of hybrid warfare. In this intervention, on the one hand, Russia has conducted successful psychological operations and communication campaigns; on the other hand, Russia has gotten support from pro-Russian forces in the region and organized its campaign on the legal ground.

Military historian Peter R. Mansoor defines hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents, and terrorists), which could include both state and non-state actors, aimed at achieving a common political purpose" (Murray & Mansoor, 2012, p. 2). Subsequently, he emphasizes that hybrid warfare consists of all levels of war, including strategic, tactical, and operational. That is to say, according to Mansoor, hybrid warfare is a comprehensive conflict in which various actors, tools, and methods contain within themselves.

*Gerasimov Doctrine*

In his famous article "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," Russian General Valery Gerasimov" dwells on the changes in the character of warfare. Gerasimov remarks that (Military Review: The Professional Journal of the United States Army, 2016, p. 24):

> In the twenty-first century, we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template… The very "rules of war" have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.

Taking into consideration the remarks mentioned above of Gerasimov, it can be said that the shape and concept of war have changed from traditional forms and methods to new forms and techniques. This new war is not limited to the states of war; it can also occur out of the war. Indeed, this new war often emerges in environments where there is no active battlefield. By means of information technologies, the war has been moved from battlefields to information spaces in which information technologies are used. As a result of this, while the effectiveness of war has increased, its cost has decreased.

Gerasimov keeps going with its remarks by attributing the Arab Spring. He says that (Military Review: The Professional Journal of the United States Army, 2016, p. 24):

> The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures—applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.

In this sense, he points out that new ways and methods have been used to achieve social, political, and economic goals. The doctrine explains how the character of war has changed.

### 2.2.3 Asymmetrical Warfare

The classical conception of war is based on the idea that wars occur between states. However, this idea has not been enough to determine the sides of the war since the Second World War. After the Second World War, the independence of some states and the establishment of new states has led to the emergence of new world order, in which new non-state actors consisting of individuals and groups influenced the international system. Following the collapse of the USSR, the effects of these actors in the conflicts have markedly been started to be felt. With the help of globalization and the facilitating accessibility to information technologies, non-state actors supported by various individuals, institutions, states, and intelligence services have become a threat for states and act as a proxy for their supporters. In this context, the world has been experienced asymmetric warfare among actors who have disproportioned force.

The term asymmetrical warfare, which has been used for several decades, is defined by Patrick M. Hughes as “attacking an adversary’s weaknesses with unexpected or innovative means while avoiding his strengths” (Hughes, 1998, p. 17). The weaker side uses non-traditional methods and benefits from technology in order to remove the imbalance between itself and the relatively powerful one. “Asymmetric approaches often employ innovative, non-traditional tactics, weapons, or technologies

and can be applied at all levels of warfare, strategic, operational, and tactical, and across the spectrum of military operations" (Metz, 2001, p. 24).

In another definition, asymmetrical warfare is described as "a form of warfare in which a non-state actor uses unconventional tools and tactics against a state's vulnerabilities to achieve the disproportionate effect, undermining the state's will to achieve its strategic objectives" (Lele, 2014, p. 103). Asymmetrical warfare is a form of conflict in which relatively weaker actors have the ability to fight against powerful actors. While doing this, the weaker actor exploits asymmetrical threats, including terrorism, insurgency, nuclear, chemical, biological, and information operations, and so, it builds a capacity to fight against powerful actors.

September 11 attacks are one of the well-known concrete examples of asymmetrical warfare. Al-Qaeda-affiliated hijackers organized four coordinated attacks targeting symbolic buildings and compounds of the United States. As is also understood from the example of the September 11 attacks, Al-Qaeda, a terrorist organization, carried out attacks to a superpower in front of the world's eyes, and as a result of this, it was successful in terms of its impact on the United States and the rest of the world. Despite its relatively weak power, it shows how a non-state actor could make an asymmetric impact on a powerful actor by benefiting from unconventional ways and unusual tactics.

### 2.3 Types of Information Warfare

Information warfare splits into five categories mainly by its content: command and control warfare, cyber warfare, psychological warfare, economic warfare, and electronic warfare. While psychological warfare, cyber warfare, and electronic warfare count on a combination of information and technology, command and control warfare and economic warfare mostly rely upon the information.

### 2.3.1 Command and Control Warfare

Command and Control Warfare is "the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities while protecting friendly command and control capabilities against such actions" (Hutcherson, 1994, p. 50). It is a strategy or policy that includes actions aimed at steering the command-and-control structures and systems. Command and control warfare is divided into two branches, command and control counter and command and control protection. In these two branches, command and control warfare is performed in five ways, so-called the five pillars of command-and-control warfare, which are operations security, electronic warfare, psychological warfare, military deception, physical destruction (Hutcherson, 1994, p. 50). With the help of these pillars of command-and-control warfare, it is strived to affect the enemy's decision-making process by destructing and exploiting it. Command and control warfare and the other types of information warfare are mostly intertwined with each other and have various interactions with one another in the information environment.

C2W affects command and control ability constituting nine prerequisites: knowledge and experience, operational picture, trust, information flow, situational awareness, objectives, feedback, flexibility, and decision making (Hammervik, Lindoff, Castor, & Tydén, 2007). These are the necessity for the ability of command and control, and if one of those prerequisites are destroyed or disrupted, this brings about a negative impact upon command-and-control structure. That is to say, C2W includes actions intended to disrupt the enemy's command and control ability while protecting friend ones.

The prototype of command control warfare is seen in Operation Desert Storm in Gulf War (January 17, 1991-February 28, 1991) (Struble, 1995, p. 91). In this operation, the administrative ability of the Iraq army was deactivated by being assaulted by its command-control systems, communication networks, and sensor installations. In conclusion, a new approach to the conduct of the war has been

introduced that the destruction of the administrative ability of the enemy is more effective than the destruction of the enemy forces.

Benefiting from Clausewitz's concept of the centre of gravity, John Warden, architect of the Gulf War air campaign, analyzed the enemy as a system and developed a model named five strategic rings consisting of five intertwined circles (Fadok, 1995, pp. 24-25). Warden prioritized from innermost to outmost as leadership, organic essentials, infrastructure, population, and fielded forces. Leadership is the centre of the model and consecutively encircles the other circles. If the leadership exposes to any damage or neutralize, then the other circles will impact from that. According to the model, the most effective strategic plan should target the leadership. If this is not within the bounds of possibility, it should focus on the ones that influence the mind of the enemy. In other words, while the destruction of the centre of the leadership will completely neutralize the system, the attacks on other circles will create psychological pressure on leadership. In both situations, the functionality of command-and-control ability is damaged.

### 2.3.2 Psychological Warfare

Psychological warfare is based on wetware operations that are the most complex information operations and part of PSYOPS. It focuses on the human mind in the information environment. In this type of information warfare, the whole activities aim to change, direct or shape the minds of individuals, groups, a specific population, or large masses.

One definition of psychological warfare is "the planned tactical use of propaganda threats, and other non-combat techniques during wars, threats of war, or periods of geopolitical unrest to mislead, intimidate, demoralize, or otherwise influence the thinking or behavior of an enemy" (Longley, 2019). Due to its nature, psychological warfare is an invisible and intangible yet perceptible battlefield. Thoughts, minds, and behaviors are observed to be affected by various psychological actions consisting of non-combat methods during either wartime or peacetime. Considering today's ever-evolving technological conditions, it is evident and

noteworthy how much psychological warfare can penetrate the information environment.

Psychological warfare includes strategic, tactical, and provocative aims. In the strategic purpose, psychological warfare, a large mass including both friends and the hostile population, is directed to be achieved specific objectives with the help of the applications of psychological operations. In the tactical purpose of psychological warfare, a target population is directed if required at achieving objectives. As for provocative purpose psychological warfare, the target population is provoked for sedition by manipulating their beliefs, weaknesses, vulnerabilities.

Understanding the culture, religion, economic situation, vulnerabilities, strengths, and weaknesses of the target population and gathering information regarding such issues is crucial for conducting psychological operations. In view of this information, the target population is tried to be influenced by imposing upon them intended thoughts in order to misguide them in line with specific ideas. Directions implemented on the target population sometimes are in the shape of intimidation, discrediting, humiliation, and sometimes are deceptive, disinformation, and misinformation.

Due to ever-growing mass communication in the modern world, the execution areas of psychological operations have a vast area that is constantly expanding and evolving. These actions are seen at any moment in any interaction. In particular, the emergence of social media has taken this interaction into a further dimension. Social networks such as Twitter, Facebook, WhatsApp, and YouTube have removed the distances among people who live at different places far from each other over the world. In this way, people have had the opportunity to easily exchange ideas and get in contact with each other even from remote locations. They can quickly become organized, orchestrate any event, or arrange any meeting through social media networks. The Arab Spring is one of the most well-known cases in point of such an organization in recent years. The people who participated in the 2011 Egypt Uprising drew advantage from social media platforms. They organized the January 25 protest by benefiting from Facebook: thus, they provided simultaneous mobilization in the recruitment, planning, and coordination process (Clarke & Kocak, 2020, p. 1032).

On the other hand, the usage and manipulation of social media and internet platforms alongside traditional media by terrorist organizations reveal a significant concern in terms of national or international security. Terrorist organizations use these platforms with the intention of intimidation, creating fear and social unrest. Furthermore, they spread their ideology, beliefs, ideas, and narratives through social media and entice more followers in order for recruitments in a short time.

*Propaganda*

Propaganda is all kinds of work that aims to affect the minds of a certain community or large masses. This effect is not on behalf of the target population; it aims to direct them with distorted information and embed intended ideas and thoughts into their minds. There are three types of propaganda; white propaganda, grey propaganda, and black propaganda.

Adolf Hitler effectively used propaganda before and during World War II, and Hitler achieved to affect the mass population through his discourses. Hitler appointed Joseph Goebbels, who was one of his closest colleagues, as Reich Minister of Public Enlightenment and Propaganda. Goebbels conducted propaganda actions on behalf of Hitler, and he had complete control of German media. He regulated German media in line with Nazi Party's (Nationalist Socialist German Workers' Party) ideology, and on the other side, he created hatred against Jews population.

Propaganda is classified into three categories regarding the acknowledgment of the source and accuracy of information: white propaganda, grey propaganda, and black propaganda (Jowett & O'Donnell, 2015, p. 20).

→ White propaganda is the type of propaganda in which the source is obvious, and propaganda actions are explicitly managed. Even though white propaganda is ostensibly predicated on accurate knowledge, it does not display the whole truth. The main point of white propaganda is to proffer selected and extracted reality to the audiences for a predetermined purpose.

→ Grey propaganda is the type of propaganda in which the source is not precisely clear and visible. Inverted and falsified information is interspersed among correct ones. In this way, it tries to deceive the target society and blur the environment by eliminating the line between truth and wrong.

→ Black propaganda is the type of propaganda where the source is not overt or displayed as revealed. However, this source is deceptive, and the actual source primarily serves the purpose of the other party. Compared with white and grey propaganda, black propaganda is the most dangerous type of propaganda. It lays on fake, distorted, inverted information and includes immoral practices such as defamatory campaigns, all kinds of lies, and slander.

*Disinformation and Misinformation*

Briefly stated, disinformation is consciously misdirecting a certain target group or masses by giving incomplete or incorrect information and thereby creating information pollution to prevent reaching the correct one (Dictionary.com, 2020). There is some deception. It penetrates public opinion. Disinformation is one of the methods of psychological warfare and is benefitted from it in many fields, from politics, economics to intelligence.

The most important feature distinguishing misinformation from disinformation is inadvertently spreading false or inaccurate information because the false or inaccurate information is believed to be accurate (Dictionary.com, 2020). There is no deliberation. Misinformation, another method of psychological warfare, brings about information confusion and disorder in the information ecosystem.

*Demoralization*

Demoralization is one of the exercises of psychological warfare and its purpose is to get the enemy down by generating despair (Military Wiki, n.d). Especially in a time of war or in a state of tension, people are more likely to be dismayed or despair.

In order to demoralize the target audience, psychological warfare means such as propaganda, disinformation, and deception is employed. Demoralization necessitates a process in which the target audience is exposed to some psychological actions. In this process, visual, written, and auditory media channels are activated to be able to keep the target audience under psychological pressure by sowing the seed of fear and anxiety in them. Consequently, the target audience is filled with sentiments of insecurity, anxiety, and inability to predict the future. This sense deprives people of taking pre-emptive actions and of resistance against applied demoralization campaigns.

*Strategic Communication*

Communication is a concept that describes sharing of emotions, opinions, decisions, and information among individuals, while strategic communication is a modality consisting of a planned and organized sharing of these assets. The term strategic communication is mainly defined as "the purposeful use of communication by an organization to fulfill its mission" (Hallahan, Holtzhausen, van Ruler, Verčič, & Sriramesh, 2007, p. 3). In order to clarify, strategic communication aims to control and change opinions, thoughts, and emotions by giving purposeful information through communication tools in line with objectives. And also, it is a process in which it struggles to influence behaviors and perception of the target population.

Different from misinformation and disinformation, the target audience is exposed to designed and intended information in line with missions in strategic communication. That is to say, disinformation and misinformation are about the intentional and non-intentional dissemination of false information, while strategic communication is related to spreading the desired information to the intended population.

Together with ever-growing and developing technological innovations, today's sophisticated and complex world order, which involves various intertwined actors consisting of individuals, governments, industries, special organization groups, postulate a strategic communication among these entities that present using integrated,

holistic messaging to contact disunited population through communication tools (Holtzhausen, Fullerton, Lewis, & Shipka, 2021, p. 6). Public relations, advertising, integrated marketing communication, journalism, and organizational communications have formed the foundational disciplines of strategic communication, and strategic communication has also been practiced in different domains from management communication, information\social marketing campaigns, financial communication, health communication to public diplomacy (Holtzhausen, Fullerton, Lewis, & Shipka, 2021, pp. 6-12). Furthermore, due to the facilitation of accessing the information technologies and globalization, NSAAs, like terrorist organizations as illegal entities, have also benefitted from these assets and paid attention to strategic communication in their unconventional warfare.

Effective strategic communication starts with analyzing problems or opportunities facing the organization through research, and definite goals and objectives are the basis for planning, evaluating the efforts and strategy and message development (Hallahan, Organizational goals and communication objectives in strategic communication, 2014, pp. 252-253). The essential steps for the strategic communication planning process are to determine organizational goals (such as enhancing organizational performance, influencing public policy, promoting cultural values) and communication objectives (such as voting, co-operating, supporting or participating in supportive cultural causes and activities) along with various intermediate steps (knowledge, attitudes, intermediate actions, and post-actions behaviors) (Hallahan, Organizational goals and communication objectives in strategic communication, 2014, p. 252).

Creating effective strategic communication that will help organizations achieve goals and objectives involves five tenets: 1. intentional message design, 2. correct platforms, 3. calculated timing, 4. audience selection and analysis, and 5. desired impact (Roberts, 2016, pp. 2-3). Intentional message design is a starting point for a competent strategic communication plan that necessitates carrying a concrete and realistic message to influence human behavior. Correct platforms are communication tools consisting of various assets, such as every written and visual platform, especially internet platforms, with the help of developing technology. Calculated timing means that put the intentional message of the strategic communication plan into action at the

right time when the target population is most receptive to receiving the relevant message. Audience selection and analysis signify which target audience can show interest in the intentional message and respond to the message. Finally, after activating the strategic communication plan, the desired impact measures whether the intentional message was efficient and whether the strategic communication plan was successful.

### 2.3.3 Cyber-Warfare

Cyberspace is considered the latest (fifth) domain after land, air, sea, and space (Pellerin & American Forces Press Service, 2010). It is a virtual and invisible field contrary to classic battlefields. All actions performed in this space are directed to affect computer networks, computer networking services, and other information systems. Therefore, any security vulnerability forms a basis for cyber-threats targeting these networks and systems. In this sense, numerous actors such as states, non-state actors like terrorist groups, and various spy and crime organizations attempt to harm opponents' computer networks or capture information to serve their various political, social, and economic objectives.

As a new concept of battle, cyber warfare is accepted by most that any aside, having technologic superiority and dominating computer networks will take competitive advantage upon others in cyberspace. Cyberwarfare is a kind of tactic and strategy in the virtual environment to defend and attack computer networks and information systems. To that end, a variety of cyber-attacks are organized with the intention of protection, sabotage, espionage, economic crime, information gathering, and denial of service. Information technologies dominate almost every field from social, education, health, security, finance, and transport to the military in today's world. Multiplexed applications are conducted in these fields with the help of computer networks. Taking into consideration that sphere of influence of cyberspace is far and wide, it can be understood how devastating consequences possible cyber damage could have.

Accompanied by the numerous usage areas of computer networks, one of the key areas is the usage of these networks in industrial areas. When a possible cyber-

attack on industrial equipment such as critical infrastructures, oil/gas pipelines, control systems, nuclear facilities, and other power plants is taken into account, it can be estimated how much the results of this attack on this equipment would be frightening. One of the most known cyber-attacks is Stuxnet, which is a malicious computer worm aimed at interrupting Iranian Nuclear Facilities. Having changed the nature of cyber warfare, Stuxnet was the first case in which industrial equipment was targeted with a cyber-weapon (Shakarian, Stuxnet: Cyberwar Revolution in Military Affairs, 2021, p. 1). Ultimately, the attack was successful and a significant advance in the development of malicious worms (Shakarian, 2021, p. 1). In this sense, the usage of a cyber-attack against the industrial equipment in the Stuxnet case is an example of the future cyber-attacks that would occur.

Cyberwar is "an extension of policy by actions taken in cyberspace by state or non-state actors that either constitute a severe threat to a nation's security or are conducted in response to a perceived threat against a nation's security" (Shakarian, Ruef, & Shakarian, Introduction to cyber-warfare a multidisciplinary approach, 2013, p. 2). On the one hand, an aggressor tries to manipulate, destroy, and damage the network-centric entities of an opponent side in cyberspace and exploits from these entities if required; on the other hand, the defender exposed to attack tries to protect itself or carried out a counterattack to the aggressor.

Apart from other fields, cyber technology is used on a large scale in the military domain. "Whether through military equipment and weapons systems, satellite and communications networks, or intelligence data, armed forces are highly dependent on information and communications technology" (Cornish & Yorke, 2010, p. 6). As the usage of cyber technology by an actor in the military domain increases, it cannot be thought military equipment without technology in this age. The dependency and vulnerability of the actor to this technology increases in proportion to the use of cyber technology.

The proliferation of the usage of information technologies and systems also offers an advantage to non-state actors in accessing and using cyberspace actively. They have the potential to employ digital force or, to various degrees, to be involved in cyber military operations (Nicolò Bussolati, An Essential Classification of Non-

State Actors Operating in Cyberspace chapt, para. 1, 2015). Therefore, the ability of non-state actors to use cyberspace has increased the probability of cyber threats which to come from these entities to states.

Cyber technology has gained ground in terrorism. Damaging cyber-attacks on people or governments with the intention of social and political take place within the scope of cyber terrorism. These attacks have the aim of intimidation and creating psychological pressure on the target group. “A cyber-terrorist might hack into computer systems and disrupt domestic banking, the stock exchanges, and international financial transactions, leading to a loss of confidence in the economy. Alternatively, he might break into an air traffic control system and manipulate it, causing planes to crash or collide. A terrorist could hack into a pharmaceutical company’s computers, changing the formula of some essential medication and causing thousands to die. Or else, a terrorist could break into a utility company’s computers, changing pressure in gas lines, tinkering with valves, and causing a suburb to detonate and burn” (Goodman & Brenner, 2002, p. 150).

To sum up, the utilization of cyber technology as a concept of battle is a new matter of fact and does not go a long way back. The cyber-attacks in this issue are limited. Up until today, any noteworthy cyber-attack has not existed; however, the likelihood of accruing large-scale or coordinated cyber-attacks together with developing technology in terms of cyber warfare is an undeniable fact for the future.

### 2.3.4 Economic Warfare

Economic Warfare is one of the types of Information Warfare. The economy is all actions aiming to meet needs and comprise a large field ranging from production, consumption, import-export, transportation to distribution. In case of some of the deterioration in one of these fields, it will inevitably have a negative impact on the entire economic system. Moreover, the nature of the economy intertwined with social and politics reveals a different problematic point which the negative impact affecting the entire economic system also expands on social and political areas. This inference is an indication of how any deterioration in an economy would create a domino effect

in other areas. From this point of view, one of the best ways of disrupting the enemy's unity without creating a de facto war situation is to paralyze or damage its economic system.

"Economic warfare refers to the conscious utilization of economic assets to advance national interests and national power vis-a-vis adversaries in overt hostilities" (O'Leary, 1985, p. 185). Economic warfare does not have a concrete battlefield. The main objective is to neutralize the adversary's economic and financial systems by using several tools of the economy. Compared with conventional war, economic warfare has lower cost, less risk, and serves the aggressor's purpose providing rapid collapse of the enemy's economy.

Libicki attributes to Economic Warfare's marriage with Information warfare could take two forms: information blockade and information imperialism. He assumes that the welfare of societies will be affected by information flows due to the efficacy of information blockade, and nations would strangle others' access to external data. Consequently, cutting off access would cripple the economies of those nations. He perceives trade as war, and nations struggle with one another to dominate strategic economic industries.

Considering the economic warfare, for the sake of an example, the United States' economic warfare against Iran is one of the best-known, which is still ongoing. The tension between the United States and Iran began four decades ago when Iranian Revolution erupted in 1978-79. Since then, the sanctions on Iran's economy applied by the United States continued from time to time by intensifying, time to time by abating. As of 2018, the severity of these sanctions has reached such a position that the military confrontation between the United States and Iran is no longer a remote possibility.

Economic warfare is a strategy aimed at subverting the economies of rival parties by wielding a variety of economic actions. The hallmark of economic warfare is to be obtained a quick and effective result as long as the proper economic means are operated and these economic actions conducted are successful. The main tools of economic warfare are embargoes, boycotts, blockades, sanctions, economic strikes, tariffs, export control.

In today's modern world, technology, together with globalization, makes the states, corporations, or other industrial powers extremely vulnerable against any unfavorable impact due to ever-increasing interconnections, interdependences, and mutual interactions among these actors. This fact makes information acquisition essential for reciprocal parties about each other's economic situations, structures, and systems in terms of both defensive-aimed and offensive-aimed. The parties use the information obtained in line with their own economic warfare purposes.

Economic warfare is generally based on three main purposes; economic, political, and military.

→ Economic warfare in terms of economic-purposed divides into five categories: "guaranteeing sources of supply, guaranteeing markets, improving the terms of trade, denial, and economic takeover" (Allen, 1959, p. 261). The first three of these categories portray a regular flow in an economy, and there are no requirements for economic warfare. Nevertheless, others address a negative course and a process that means a kind of economic war.

→ Military-purposed economic warfare has two dimensions: one is that economic warfare regards as a subsidiary action for military operations; the other is related to the use of economic warfare for the peacetime military establishment and the preparation of war (Allen, 1959, p. 260).

→ Political purposed economic warfare is waged for the acquisition of political advantage. The desire for respectability and status, the takeover of another country through economic influence and a concrete specific fashion, for instance; the desire for making a unique alliance, the obtaining the vote of another in some international organization, and the eliminating a particular political or military leader in domestic or foreign policy comprise a basis for political-purposed economic warfare (Allen, 1959, p. 262).

### 2.3.5 Electronic Warfare

In the information age in which we have lived, the effect of information and communication technologies has gradually been felt in all areas, from social, economic, military, to scientific. These technologies have enabled new technological systems and equipment to enter various fields. Accordingly, new techniques and gear based on information and communication technologies have emerged in the military area. With the introduction of these technologies into the military field, the concept of warfare has moved to a new dimension where traditional methods and high technology are predominantly used, and the character of warfare has changed. The electronic systems and equipment of warfare based on the electromagnetic spectrum in the information age have played a crucial role in determining the course of events. Therefore, having such tools as drones, missiles, reconnaissance and surveillance tools, communication satellites and systems, space weapons, nuclear weapon systems, command and control systems has been a necessity in order to achieve various objectives and gain a relative advantage over others.

"The term electronic warfare refers to military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy" (Homeland Security Digital Library, 2007). Electronic warfare is actions in the electromagnetic spectrum that aim to reduce or avoid the usage of the electromagnetic spectrum by hostile powers and provide benefits from the electromagnetic spectrum to friendly forces. Electronic warfare, which is a technical form of warfare, is conducted in both wartime and peacetime. Electronic warfare is examined in three subdivisions: Electronic Support, Electronic Attack, and Electronic Protection.

*Electronic Support*

"Electronic Support refers to the division of electronic warfare involving actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition,

targeting, planning, and conduct of future operations" (Joint Publication 3-13.1: Electronic Warfare, 2007). In this subdivision of electronic warfare, it aims to get under control of the electromagnetic environment against hostile powers' actions. The acts of Electronic Support are performed passively and include all activities used to collect information. Electronic Support actions are executed in two ways: the first is to provide information that comprises the acts of identification, analysis, detection, and the second is intelligence, which consists of the activities related to electronic and communication.

*Electronic Attack*

"Electronic Attack refers to the division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires" (Joint Publication 3-13.1: Electronic Warfare, 2007). Electronic Attack includes a variety of actions aimed at attacking the electromagnetic spectrum used by the enemy. These actions are carried out actively and passively, and it is aimed to block and degrade the enemy's usage of the electromagnetic spectrum by restricting and misleading it. On the one hand, the type of active Electronic Attack, it is commonly benefited from electromagnetic jamming and deception. On the other hand, in the type of passive Electronic Attack, chemical and mechanical systems are used in order to impact the target.

*Electronic Protection*

"Electronic Protection refers to the division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the electromagnetic spectrum, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability" (Joint Publication 3-13.1: Electronic Warfare, 2007). Electronic Protection systems

purpose to defend friendly electronic systems from electronic threats and hostile systems and neutralize them before they are not generated any damage to friendly systems. In this subdivision of electronic warfare, it is tried to provide a protective shield by managing and strengthening the electromagnetic spectrum and controlling the emission.

# 3. THE INVOLVEMENT OF THE ISLAMIC STATE OF IRAQ AND SYRIA IN INFORMATION WARFARE

ISIS was a salient terrorist organization with its featured out-of-the-ordinary character in the capacity to use information, especially between 2014 and 2016. Embraced the extreme radical ideology of *Salafi* Islam, the organization also had adopted the new war concept that harbored asymmetric and hybrid methods in the framework of information warfare by trying to use information technologies to the utmost. In this manner, mainly five types of information warfare were tried to integrate into the information warfare of the organization to measure the information warfare capability; Command and control warfare, psychological warfare, cyber warfare, economic warfare, and electronic warfare. Each type of information warfare found a place in that of ISIS to a certain point. However, while having more success in some, others had an unsatisfactory level of achievement. While ISIS succeeded in the information warfare capability of on few types, it was not fairly clear to mention a complete achievement.

The placement of types of information warfare on those of ISIS established a different vantage point in terms of how a terrorist organization could manage the concept of information warfare as an illegal entity. The environment of confusion and restlessness caused by war and conflict since the Soviet Occupation of Afghanistan in 1979 gave rise to be brought up experienced and knowledgeable individuals subject to military information in the geography where ISIS would later gain dominance. The terrorist organization established by these individuals became a competent entity that left a trace in history by benefitting from the technological advancements and the facilitation of access to information technologies that made an outstanding contribution to the ability of ISIS to handle the information warfare concept.

## 3.1 The Islamic State of Iraq and Syria as A Non-State Actor

Non-State Armed Actors are individuals or groups that use violence as a method and act independently of states for social, political, and economic purposes. While

some actors or groups such as criminal organizations and private security companies carry economic objectives in the establishment, the groups like militias, guerillas, and terrorist organizations convey social and political objectives such as ideological, ethnic, and religious. Even though these entities are independent of states and their governments, they are also known to get support from different states and their organizations.

The history of NSAA dates back to ancient times. Sicarri, one of the earliest known terrorist formations, was a robber group that carried out assassination assaults against Romans and their supporters in Jerusalem (Hengel, 1989, pp. 46-47). The rising of today's NSAA goes back to after the World War II period when some countries gained their independence. This situation caused discontent and strife among some different religious and ethnic groups. In reaction to this, disgruntled individuals and groups have begun to step into action for the sake of their interests. Following this, alterations of the nature of war and security in conjunction with the facilitation to access information technologies have caused asymmetric and hybrid warfare environments to emerge that housed many terrorist and paramilitary groups after the post-Cold War era. In addition to this, the disputes have exceeded battlefield borders thanks to the use of information technologies such as telecommunication and computer systems, networks, and electronics devices.

In recent decades, the effects of the NSAAs in the international area have been started to be seen more than ever before. The ease of the accessibility to information technologies by NNSAs has brought them to such a level that they could be able to compete with the states in terms of information warfare capability to a certain extent. Besides, they have gained support from various states and become a proxy tool for these states in asymmetrical and hybrid warfare pitches. Therefore, the supporting of the NNSAs by various states or global powers desiring to profit from conflicts has led to proxy wars in battlefields and combat zones.

As an NSAA, the emergence of ISIS and its regional and cross-continental actions have left their mark in history. The organization became the most formidable terrorist structure on short notice. After a couple of days of fighting between ISIS and the Iraqi Security Forces, the fall of Mosul on June 10, 2014, had astonished the whole

world at the success of ISIS. ISIS pursued both a hybrid strategy and became a part of asymmetric warfare by utilizing conventional and non-conventional methods based on information technologies.

### 3.1.1 The Overview of ISIS

The foundation of the Islamic State dates back to the end of the nineties. It has become an extremely sadistic, savage, and tyrannical terrorist organization compared to its equivalent organization such as the Taliban and Al-Qaeda. By committing horrendous assaults and acts, especially as of 2013, the terrorist group has managed to attract the whole world's attention to itself.

Islamic State of Iraq and Syria (ISIS), also known interchangeably as Islamic State of Iraq and Levant (ISIL), also known as the Islamic State, and also known in Arabic *ad-Dawlah al-Islāmiyah fī' l-ʿIrāq wa-sh-Shām (Daesh)* is a jihadist terrorist organization. ISIS has the *Salafi* -jihadist ideology of Sunni Islam that teaches about why and how the fight (Hashim, 2019, p. 22). Besides, the theology and method of the Islamic State are bound up with Wahhabism, where religious innovation is weak and external cultural influences on religion are not adopted (McCants, 2015, pp. 150-151). ISIS's primary goal was to establish an Islamic caliphate on the basis of *Salafi* ideology and expand its occupied territories to Muslim countries to unify under the supreme caliph and rule them by Sharia Law. To this end, ISIS has leaned its strategy on a fundamentalist, tyrannical and irreconcilable approach for the sake of the establishment of its caliphate.

The founder and the first leader of ISIS are Abu Musab al-Zarqawi. Zarqawi arrived in Iraq in 2002 with its initial organization called *Jama'at al-Tawhid wal-Jihad (JTJ)* that had founded in 1999 with an inadequate system of hierarchy and management and lack of a base for operations, military credentials, and support (Hashim, 2019, p. 25). Following the death of Zarqawi on June 6, 2006, and the establishment of the Islamic State of Iraq in October 2006, Abu Ayyub Al Masri, also known as Hamza Al- Muhajır, took over the leader of the Al-Qaeda in Iraq, while Abu Omar Al- Baghdadi became the first leader of Islamic State of Iraq (Al Qaeda in Iraq

leader Abu Ayyub Al- Masri pledged allegiance to the Islamic State of Iraq in November 2006) until that time both of leaders were killed in 2010 as a result of a joint operation of the US and Iraqi forces (Tønnessen, 2015, pp. 49-50). After the death of Abu Ayyub Al-Masri and Abu Omar Al- Baghdadi, Abu Bakr Al-Baghdadi, who was well-versed in the knowledge of Islamic history and ancestral studies, became the leader of Islamıc State on May 16, 2010 (Alkaff, 2014, p. 5), until he died during an operation by the US special forces on October 27, 2019 (BBC News, Trump: 'Abu Bakr al-Baghdadi is dead', 2019).

ISIS had a highly systematic leadership structure that emanated from horizontal and linear echelons. In this sense, the caliph was the head of these echelons and had absolute authority over the whole network. A cabinet that consisted of the caliph's advisers was directly tied to the caliph. Also, there was two vital body of the network; the *Shura* council/ministry that served as the decision and policy-making body, and the Sharia council that interpreted sharia law and other religious affairs. Under the caliph, Iraq and Syria were divided into two governances led by two deputy leaders of the caliph, and beneath these deputies, the administration split into several councils: Military Council, Security and Intelligence Council, Religious (Affairs) Council, Finance Council, and Media Council.

ISIS was born in Iraq. The first operational location of the organization had become Iraq. Then, Bashar al-Assad was condoning to the members of ISIS crossing in Iraq and Syria a resultant environment of instability in Syria following the Arab Spring, so this gave an opportunity to ISIS's sprawl in Syria. And then, ISIS expanded its impact from Iraq and Syria to more than 70 other countries.

The members of ISIS consisted of both local and foreign fighters. Especially in Iraq, due to internal turmoil, insufficiency of public services such as education, transportation and infrastructure, healthcare and social services, as well as poor economic conditions, the local community had considered ISIS to be the lesser evil and conceded ISIS dominance. Local people made up the majority of ISIS fighters in Iraq for the reasons such as money, power, and religious ideology.

Foreign fighters were people who were not citizens of conflict states but participated in the conflictual riots in those states. Compared to local fighters, foreign

fighters participated in ISIS principally on the ground of jihadist ideology. Although foreign fighters participated in ISIS for social, political, or economic reasons, many foreign fighters coming from countries with high levels of economic development demonstrated that these fighters were likely driven by ideology rather than by economic and political conditions (Benmelech & Klor, 2020, p. 20). The great majority of ISIS members came from the Middle East and Arab countries; many of them also came from Western nations, Russia, Indonesia, and Tajikistan (Benmelech & Klor, 2020, p. 1).

### 3.1.2 The Reasons for The Rise and Spread of ISIS

The September 11 attacks in 2001 and the ensuing chaos and instability environment gave cause for the rising of the Islamic State. Additionally, the emergence of the Syrian Civil War exacerbated the tensions in both states, and this situation contributed to the spreading of the Islamic State. The main five reasons for the rise and spread of ISIS were the US invasion of Iraq, Sectarian Conflict in Iraq, the policies of Nouri al-Maliki, Baathists, and the Syrian Civil War.

—*The US invasion of Iraq*

September 11 Attacks in 2001 have opened the doors of a new era for the whole world. The concept of war on terror, the first time announced by George Walker Bush, who was the 43rd president of the United States, entered the international literature. The United States invaded Iraq in 2003 on the pretext that Iraq has Weapons of Mass Destruction (WMD) and cooperates with Al-Qaeda. In the wake of the US invasion of Iraq, the chaos caused by the invasion gave rise to the grievances of the Iraqi people who were already suffering under Saddam's regime to deepen. The people of Iraq became open to foreign intervention. Especially Iran, of which population mostly consists of Shiites, began to rule over Iraq by using Shiite fractions. The strengthening of the Shiites and the spread of the Shiite's influence over Iraq led to the beginning of the Sunni insurgency because of the Shiite's oppression and violence against Sunnis.

This situation brought about the emergence of jihadist terrorist organizations ISIS and the like.

—*Sectarian Conflict*

The political structure of Iraq in the post-occupation was shaped on the sectarian axis. The invasion resulted in the Shiites, who had barely any influence on Iraq policy, economy, and social fields in the Saddam era, becoming the dominant power after the US invasion. Contrary to Shiites, Sunnis and their Baathist associates were excluded from Iraqi politics. As a natural consequence of this, a Sunni insurgency commenced against the Shiite government and its Shiite affiliations.

— *The Policies of Nouri al-Maliki*

Sectarian and authoritarian policies implemented by Iraqi Prime Minister Nouri al-Maliki pushed the Sunnis off the Shiite-dominated government and prompted them to revolt. Peaceful protests starting in December 2012 converted into armed resistance because of that Nouri al-Maliki did not accede to compromise with protesters, and also Iraqi army slaughtered more than fifty of them by carrying out a raid on protesters in a peace camp in Hawija in April 2013 (Cockburn, 2014, p. 47). This played an essential role in the acceptance of ISIS by the Sunnis.

—*Baathists*

After the invasion and toppled down Saddam's Baathist Regime, thousands of Baathist officers had been arrested in detention facilities by the United States or dismissed. With their knowledge, experience, and military skills in the Iraqi army, these Baathist officers had supported Sunni insurgencies and played a crucial role in establishing the Islamic state. Additionally, they had been powerful actors in the rise and expansion of the Islamic state. Moreover, these former Baathist officers took part in most of the leadership cadres at ISIS's command and control structure.

*—Syrian Civil War*

The unstable environment in Syria after the Arab Spring and Bashar al-Assad's ill-advised policies towards this situation caused some states and their affiliations to interfere in Syria and many terrorist groups and their different factions to occur. As a result of this, ISIS took such an opportunity that ISIS fighters freely moved back and forth between Iraq and Syria borders; the group expanded in Syria and declared Raqqa on the Euphrates River in the north of Syria as the capital of the caliphate. The members of ISIS chased to reshape the world towards their interests by resorting to violence (Cockburn, 2014, p. 8). The amalgamation of the extremist religious beliefs and military dexterity of the ISIS movement was a result of the US occupation of Iraq in 2003 and the War that came out in Syria in 2011 (Cockburn, 2014, pp. 8-9).

### 3.1.3 The Global Coalition to Defeat ISIS

The ferocious assaults, inhumane and tyrannical activities of ISIS, and the strengthening with each passing day forced the international community to take precautions against the terrorist group. US Department of State published a statement on its website, explaining that "ISIS continued to commit crimes and violates human rights, such as the killing of civilians, mass executions, kidnapping, forced people to emigrate, mutilating children, rape, and cruel atrocities, and thus it presented a global terrorist threat," by declaring the formation of an extensive international coalition to defeat ISIS on September 10, 2014 (United States Department of State, About Us – The Global Coalition To Defeat ISIS, 2014). In that manner, it put forward the five lines of efforts; providing military support to its partners, impeding the flow of foreign fighters, stopping financing and funding, addressing humanitarian crises in the region, and exposing true nature (United States Department of State, About Us – The Global Coalition To Defeat ISIS, 2014). The U.S.-led coalition, which had around 10.000 Americans, 8.000 troops, and more than 1.600 contractors at the peak of the fight, fought against ISIS in Iraq and Syria and lost at least 74 of its fighters since 2014 to March 2019 (Sune Engel Rasmussen & Rasmussen, 2019). The U.S-backed forces thwarted ISIS from its last outpost in Syria in 2019, and ISIS turned from a terrorist

extremist group into a guerrilla insurgency group at the end of a five years U.S-led coalition campaign (Sune Engel Rasmussen & Rasmussen, 2019).

## 3.2 Placing The Information Warfare in Warfare of ISIS

The leading five types of information warfare, command and control warfare, psychological warfare, cyber warfare, economic warfare, and electronic warfare, were a basis for understanding the capability of ISIS's modus operandi towards information warfare. In order to analyze what ISIS's information warfare capability was, placing these types of information warfare into ISIS's way of information warfare provided insight into how ISIS managed its information warfare and what ISIS's information warfare capability was.

### 3.2.1 Command and Control Warfare of ISIS

ISIS had a command-and-control structure predicated on a caliph who was a religious and political leader with full authority and outrightly held powers reins. Given that command and control ability hinge on nine prerequisites by its nature of C2W; knowledge and experience, operational picture, trust, information flow, situational awareness, objectives, feedback, flexibility, and decision making, to examine these prerequisites on ISIS whether they were convenient with ISIS's was essential for the understanding of the command-and-control ability of it.

#### *3.2.1.1 Knowledge and experience*

ISIS's command and control structure emerged with US-run prisons. Many of the jihadist commanders spent time in these prisons and contacted like-minded individuals, which provided them an opportunity to expand their networks (Gerges, 2016, pp. 132-133). The leaders of the organization did time in these detention centers came to the fore on jihadist ideology. They contacted other militants who were against

the American occupation, the Shiite government, and its fractions. The incendiary effect of the Sunni resistance and a desire to establish an Islamic State commenced in these prisons. Ultimately, the superiors of this terrorist organization had come together in these prisons, engaged with other militants, and then became organized in line with a common purpose.

Rulers of ISIS spent time in US detention centers, Camp Bucca in the vicinity of Umm Qasr port city, Camp Cropper at the near Baghdad International Airport, and Abu Ghraib prison western outskirts of Baghdad in Iraq, during the American invasion of Iraq (Chulov, 2014). Nine members of the ISIS's top commands were in jail at Camp Bucca, and apart from Abu Bakr al-Baghdadi, Abu Muslim al-Turkmani, who was governor of territories dominated by ISIS in Iraq and the leader's number two, as well as Haji Bakr, who was a senior military leader, and leader of foreign fighters Abu Qasim (Kassem) were incarcerated at Camp Bucca (The Independent, 2014). Camp Bucca housed up thousands of former Baathist officers from the Saddam Regime and militants who rebelled against the US invasion in Iraq. This prison put militants like Baghdadi in touch with former Saddam officers and turned into a terror academy in which provided military skills, terrorist techniques, and tactics, as well as adopted an extremist jihadi ideology and doctrine.

Baghdadi constituted a professional combat force composed of the former Iraqi army and police officers with expertise in organization, intelligence, internal security, and Chechen commanders with guerrilla warfare skills (Gerges, 2016, p. 276). He had confidence in their operational proficiency and capability of waging in urbanization terrain and conventional warfare that they had a long history of fighting with adequate combat experience and training in consequence of their participation in the Iran-Iraq War in the 1980-1988, Iraq Kuwait War in 1990-1991, the counterinsurgency in the 1980s and 1990s, and resistance against the Americans from 2003 to 2010 (Gerges, 2016, p. 21). These experienced officers had attended military academies during the Saddam Hussein Regime and were significantly influenced by military advisers from the USSR in the 1980s (Maurer, 2019, pp. 230-231). These soldiers and officers, who had sufficient technical knowledge and background both in the combat zone and in the control system, had played an essential role in the functioning of the command-and-control system of the organization. Furthermore, they took charge at the upper levels

of the leadership cadres and the decision-making mechanism of the organization structure. ISIS had multi-dimensional components that were experts in actions and methods of asymmetric assaults, terror, and chaos, that could implement acts of guerilla, rear zone, intelligence/counter-intelligence, and deception at a high level, along with personnel who knew conventional warfare techniques and tactics (Ağar, 2015, p. 385).

Furthermore, Chechens were the most dreadful warriors due to their knowledge, experience, and guerilla warfare implementation against the Russian army, and the group cooperated with Chechens due to their controlled and combat-ready nature. To give an example, Tarkhan Tayumurazovich Batirashvili, known by his pseudonym "Abu Omar al-Shishani," had been a former sergeant in the Georgian army, was one of ISIS's most senior military commanders and a member of the group's elite *Shura* Council, and headed group's fighters from Chechnya and the Caucasus (Counter Extremism Project, n.d).

#### *3.2.1.2 Operational picture and information flow*

Being one of the Islamic State's most substantial elements, Security Council, headed by Abu Ali al-Anbari, a former operative in Saddam's Regime, held the security and intelligence affairs of the organization. *Amniyat* or security units, one of the vital organs of ISIS intelligence and counter-intelligence, developed by the former Iraqi *Mukhabarat* officers in its ranks, are responsible for raids, arresting wanted individuals, and investigating security-related cases in ISIS territories (Weiss & Hassan, 2016, p. 240). The tasks of this unit follow; "collecting intelligence for battles in Syria and Iraq, gathering intelligence about the local community, gathering intelligence about areas that ISIS intents to conquer, sending and deploying spies in other countries, gathering and analyzing intelligence about possible attacks against the Islamic state, and assassinations, kidnapping, bartering for hostages" (Speckhard & Yayla, 2017, p. 3).

*Amniyat* was sectionalized into four separate branches that each of them had its own duty; the first was *Amn al-Dakhili* with the task of ensuring security in each city,

the second was *Amn al-Askari* or ISIS military intelligence, an agency lodging the group's reconnaissance men and anatomists of enemy positions and fighting capabilities, the third was *Amn al-Kharji* or ISIS foreign intelligence, in charge of conducting espionage or plot and perpetrate terrorist operations by sending operatives behind enemy lines, and the fourth was *Amn al-Dawla*, responsible for running counter-intelligence operations, intercepting communications internally, and maintaining the organization's detention program (Weiss & Hassan, 2016, pp. 423-424).

The group had opened a *Da'wah* office which was an Islamic missionary center to gather followers; one or two men were allocated to spy/informant on their village and obtain a wide range of information related to: list the powerful families, naming the powerful individuals in these families, find out their sources of income, names and the sizes of rebel brigades in the village, find out the names of their leaders, who control the brigades and their political orientation, and find out their illegal activities (Reuter, 2015). They were liable to ascertain information as much as possible concerning target villages, individuals, groups, and the local population. In addition, these informants infiltrated into other terrorist entities, tribes, powerful families, local communities from all strata and collected helpful information for the terrorist group.

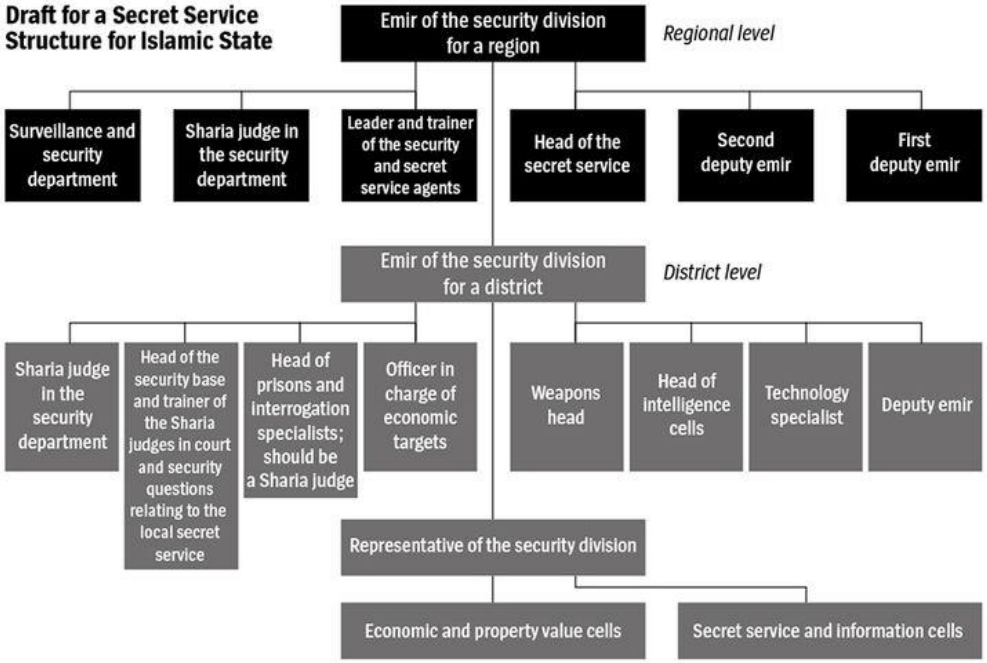


Figure 1: A digital rendering of Haji Bakr's Islamic State organigram (Reuter, 2015).

A chart is a hand-drawn organigram scratched by Haji Bakr points out a secret service/intelligence structure for ISIS (Figure-1). Samir Abd Muhammad al-Khlifawi, better known by the nom de guerre Haji Bakr, had been a former colonel in an elite intelligence unit of the Saddam Hussein Regime, came to international attention as the "architect" of the Islamic State's expansion into Syria and the man who had been "pulling strings at the Islamic State for years," were killed in Aleppo in January 2014 (Orton, 2015).

According to the chart, territories of ISIS had splinted into regions and districts, and an emir in charge of the security division for a region spearheads the whole intelligence structure of ISIS. Under the supervision of the emir, a few departments, services, and deputies subserved to the organization at the regional level, and every branch of them had particular duties and responsibilities. In the same manner, the chart portrays other emirs who administered some subgroups at the district level. The most remarkable feature of this organization chart was that the intelligence structure of ISIS had a well-organized and coordinated pattern contrary to popular opinion. Several factors, such as surveillance department, technology specialist, economic intelligence bodies, were a testament betokening how ISIS had a mighty intelligence organization.

#### *3.2.1.3 Confidence/Trust*

The inner circle of ISIS was made up of one hundred percent Iraqis, and Baghdadi did not approve of any other nationality due to his distrustfulness (Gerges, 2016, p. 150). These circles had adequate knowledge about rules of engagement, the situation, capacity, and experience of the command-and-control environment. The commanders of ISIS were able to plan, prepare, and conduct their operations and attacks independently in their respective areas of responsibility by courtesy of the military council since Baghdadi posed confidence in their qualities and ability to manage tasks (Maurer, 2019, p. 232). ISIS was a terrorist organization bringing together former Saddam Hussein's officers and other Jihadi militants who revolted against the American occupation and *Shite* groups. To this respect, the liaison between these two groups could culminate in decomposition as a consequence of a social disagreement, contradictions, disputes, and lack of confidence among them.

On the other hand, ISIS relied upon information technologies to a large extent to fulfilling its objectives. The methods applied and technology used in its control system impact on minds of ISIS sympathizers. The group had the ability to control and direct its followers from every part of the world by utilizing social media and other internet platforms. For example, the leader of ISIS had published an audio message lasting twenty minutes in which he called on Muslims worldwide to flock to a new caliphate where it had declared on Iraq and Syria soils (Al Jazeera, 2014). Such statements influenced ISIS followers, and thus, numerous foreign fighters flocked to Raqqa, the so-called capital of the caliphate, and settled there with their families.

#### *3.2.1.4 Situation awareness*

Leader cadres of ISIS had a correct understanding of their situation. Most of them had been former Baathist officers of Saddam Hussein's army, intelligence, and police officers forming the inner circle of ISIS (Gerges, 2016, p. 276). In the wake of the invasion of Iraq, these officers had been imprisoned in detention centers like Camp

Bucca, which became a training camp for Islamic extremism and jihadist ideology (Gerges, 2016, p. 133), and they were able to outline a joint plan against the American occupation and *Shite* groups. Determination of the foundation of an Islamic State ruled by Sharia Law under a caliph, the opinion that the unity of the World Muslims, and for this cause, the formation of a highly organized command and control system pointed out how much aware the group's rulers were of the situation they were in, and they had self-conscious wisdom.

#### *3.2.1.5 Objectives*

The objectives conveyed by ISIS were clear. ISIS desired to establish an Islamic caliphate based on *Salafi* ideology and broadened its boundaries to Muslim countries to unify them under the supreme caliph. In line with this purpose, ISIS followed four strategic objectives; establish a caliphate in Iraq and Levant, control and govern the caliphate, expand Islam and Sharia Law worldwide, and recreate the power and glory of Sunni Islam (Siebert, von Winterfeldt, & John, 2016, p. 15). ISIS strived to earn money and generate resources to meet the populace's needs in its dominant areas and obtain weapons and ammunition to actualize these objectives.

A hadith in Islamic eschatology attributing to the Prophet Mohammad regarding a battle of the end of days between Muslims and Christians in *Dabiq*, a town in rural Aleppo in Syria, lied behind the legitimacy and mobilization of ISIS. The fact that the name of ISIS's propaganda magazine was *Dabiq*, was not a coincidence but an indication that ISIS anticipated such a battle. In this respect, ISIS took a form of brutal, tyrannical, fundamentalist structure in that it aspires to drag its enemies into the end of times at *Dabiq*.

#### *3.2.1.6 Feedback*

The terrorist actors might neglect to receive adequate feedback from their command-and-control system because they were disposed to actualize resounding actions that resonated among the people and harm their enemies as much as they can.

The leadership cadres of ISIS considered reactions from worldwide in organizing actions as its modus operandi. The group desired to devise a mighty image. In this manner, the group tried to create a worldview that showed how ISIS was an omnipotent and tremendous organization by embarking on hybrid and asymmetric warfare strategies and tactics as well as conventional warfare ones (Wood, 2015). It aimed to create shock and awe on large masses as a requirement of its fundamentalist and tyrannical strategy. ISIS focused on receiving feedback from the international arena rather than its command-and-control chain in the wake of its brutal and inhuman actions. ISIS was a global terrorist organization and had independent cells and followers of each other that acted on behalf of the group without ISIS attachment. And these different actors posed an obstacle to getting reliable feedback in the chain of command. The organization urged Muslims from all over the world to activate them to perform terrorist acts regardless of their scales by calling for jihad.

#### *3.2.1.7 Flexibility*

Members and commanders of ISIS smoothly ran across Iraq and Syria's borders, providing them a unique mobilization for organizing simultaneous operations in both countries and in a short time. ISIS had the enormous advantage of moving back and forth between the Euphrates and Tigris River valleys and northern and western Iraq and western Syria, which provided great convenience for ISIS to conduct its operations in these two countries.

- → ISIS militants connected with Al-Qaeda and Sunni tribes in the region seized control of Fallujah and Ramadi in Anbar province in Iraq less than one week after the Iraqi army and police intervened in ongoing protests against Nuri al-Maliki on December 30 in 2013 (Roggio, 2014). As a result of the clashes between Sunni rebels and the Iraqi military, the Iraqi forces had lost control of Fallujah and Ramadi, which have strategic importance, and had to withdraw from these cities.
- → ISIS forces took over Raqqa, a city in Syria on the northeast bank of the Euphrates River, on January 14 in 2014, and declared it as the capital of ISIS

(Al Jazeera Türk, 2016). Raqqa was a city that Regime forces and Syrian opponents waged war for after the Syrian Civil War in 2011. Raqqa had also so significant for ISIS that the top executive cadres of ISIS harbored in this city, and the group's foreign fighters and their families had settled down in the city after ISIS declared the caliphate (Al Jazeera Türk, 2016).

→ Launched an attack on Mosul, the second-largest city in northern Iraq, on June 6, 2014, ISIS fighters captured control of the city after four days, with a stunning victory by force numbering some 1.300 men against the Iraqi army and federal and local police which were ostensibly 60.000 strong force (Cockburn, 2014, p. 11). The group seized a considerable amount of weapons and equipment composing riffles, Hellfire missiles, aircraft, and reconnaissance drones in consequence of the scuttling of the Iraqi army from the city of Mosul by leaving behind this ammunition (Curry, 2014).

Above mentioned operations performed by ISIS demonstrated that the organization had a broad capacity to prepare, plan, manage and coordinate successful operations. Also, the organization had such a salient strategic, operational and tactical capability that it conducted actions in Iraq, Syria, and elsewhere in short periods of which was an indication of the group's ability to adapt to the way of acting based on changes in the situation.

#### *3.2.1.8 Decision making*

Technically, ISIS's decision-making and action cycles can be examined by placing them in the John Boyd OODA Loop strategy. Security and other councils serve such as observation, orientation, and action apparatuses that Security Council collects and obtains a broad scope of information regarding security, military, financial, social affairs, and other councils conduct operations and actions related to their area of responsibility. As a decision-and-policy-making body, the *Shura* council evaluated and commentated on current issues and gave advice to the caliph.

ISIS had a highly systematic hierarchical administrative structure under a caliph in which the administrative bodies were splintered into vertical and horizontal

councils. Each administrative body had decision-making authority within the scope of its duties and responsibilities; nevertheless, the highest and ultimate executive decision-making was the caliph. For example, under the military council, ISIS commanders had a massive attack and operation competency in their area of responsibility. Moreover, the Shura council, which was one of the most significant bodies of ISIS, is formed between nine and eleven of the group's senior leaders, who were appointed by the caliph on the recommendation of emirs and provincial rulers (Haniyeh, 2014). The council convoked to contemplate current affairs, critical decisions, and policymaking and recommends the caliph regarding war and peace decision making; however, the last words rest with the caliph who has direct authority over councils (Haniyeh, 2014).

### 3.2.2 Psychological Warfare of ISIS

Today, the whole world accepts that ISIS was a terrorist organization getting strength from its psychological activities and utilizing information technologies to create its psychological campaign. The organization regarded psychological operations were an integral part of its war, and it generated its own brand in psychological warfare by leaving behind other terrorist organizations in this respect. It benefitted from the internet platforms such as blogs and webpages that the group designed for its activities and other social media platforms such as Instagram, Facebook, Twitter, YouTube by keeping pace with technological innovations and providing information flow among its followers through these platforms. Through these platforms, the group tried to engrain the organization's extremist ideologies in the minds of their followers in line with their own understanding of Islam. Besides, ISIS benefited from mistakes and abuses committed by the Iraqi government and American occupiers in such a way that it induced local people to believe and acknowledge ISIS as a security blanket for them. While ISIS was managing its psychological operations, the group acted in line with its political, religious, and social aims. The political ambitions of ISIS in its psychological warfare were to accede its Islamic state (under the caliph) and its legitimacy to the whole world by drawing a mighty image through media outfits. On the ground of its religious aim, ISIS desired

to spread its *strict Salafi-jihadi* doctrines and established an Islamic State unifying the whole world of Muslims under a caliph authority. As for social purposes, the group intended to direct the masses both from the territories it had occupied and from anywhere in the world in line with its objectives, such as enlisting new members, providing information flow among supporters, generating fear and anxiety among people.

#### *3.2.2.1 The media strategy of ISIS*

The ISIS media strategy attracted the international community's attention due to its modern, unique, and technologically blended features. The group's media strategy had the appreciable capability to sustain its psychological operations in front of the international media. The objectives of ISIS media strategy is to dictate its political and religious legitimacy, to legitimize its authority in the controlled areas, to label those Muslims who against ISIS as traitors, to threaten its enemies by communicating with the people of the world, to ingrain its ideas into the minds of Muslim youths, to recruit new members/militants for organization, to infuse fear in the hearts and minds of their enemies, to communicate with other militants, supporters, sympathizers, to exhibit itself as a daring, extremist, brutal organization than anyone else (Khawaja & Khan, 2016, pp. 107-109).

##### *3.2.2.1.1 Traditional media*

ISIS had different official media bodies, such as Al-Hayat Media center that involved videos, *Dabiq* and *Rumiyah* Magazines, *Al-Furqan* Foundation, *Ajnad* Foundation, *Al-Himmah* publications, *Al-Naba* newsletter, Al-Bayan Radio, and *Wilayat* Media offices, for pursuing its various activities such as intimidation, forming an image war, informing its followers about their legitimatize state (Kadivar, 2020, p. 3). Typically, the organization carried out some of its propaganda activities through these media bodies. Via these bodies, the terrorist

group produced content regarding heroism, spreading its extremist ideology and determining potential enemies, and published them to target audiences.

The chart (Figure 2) shows an overview of ISIS media products, the themes of these products, and the target audience. The group mainly focused on audio statements, videos, magazines, *nasheeds*, and news reports in drawing its media strategy.

| Media product | Salient themes | Target audience | Image projection tools | Notes |
|---|---|---|---|---|
| Audio statements | Fighting and violence, power projection, Islamic religious messages | All Muslims, supporters/fighters, and enemies | A presentation of a clear and decisive image—through the usage of salient themes and metaphors | Changes according to circumstances |
| Videos | Violence and warfare, power and deterrence | Mostly ISIS members and supporters | As the most visual media platform, videos are used by ISIS frequently in its Image war in an attempt to promote its narrative | Emphasis is made on presenting the organization |
| Magazines | A shift from an emphasis on power projection to more religious-based messages | Mostly the organization's supporters, potential supporters, and fighters | Usage of images (both visual images and texts) in an attempt to empower the organization, attract supporters, and present a threat to its enemies | The length of the magazines allows for various messages to be promoted |
| Nasheeds | Islamic religious messages | Only Muslim audiences—fighters, supporters, and potential supporters | Heavy usage of metaphors | The messages contain many visual descriptions that assist in the creation of the organization's image |
| News reports | The reports are brief and informative presenting power projection | Western media | Pictures or infographics | The news reports try to appear objective |

ISIS: Islamic state of Iraq and al-Sham.

Figure 2: Summary of the organization's media products (Yarchi, 2019).

From time to time, ISIS released audio statements for fighting, inflicting violence, showing power projection, or relaying Islamic religious messages to all Muslims, followers, supporters, fighters, or enemies. For instance, the group released an audio statement from Abu Bakr al-Baghdadi to its followers in May 2014, in which he called for recruits around the world to fight in his land (Ellis, 2015). In another audio statement published by ISIS in May 2016, the Islamic State called for attacks on the West during Ramadan, mentioning that: "Ramadan, the month of conquest and jihad. Get prepared, be ready, to make it a month of calamity everywhere for the non-

believers, especially for the fighters and supporters of the caliphate in Europe and America" (Reuters Staff; Islamic State calls for attacks on the West during Ramadan in audio message, 2016).

Another media product that ISIS frequently capitalized on was video records which illustrated violence, power, and deterrence. On August 19, 2014, a video delivered by ISIS displayed a man dressed in black beheaded the U.S. journalist James Foley, who had disappeared on November 22, 2012, in northwest Syria, after he had read a scripted message mentioning that his real killer was America (Carter, 2014). The beheading of the Foley shocked the world. President Obama said it was an act of violence shocking the conscience of the world as a whole, and it was revenge for the U.S airstrikes on ISIS fighters in Iraq (BBC News, Foley beheading video shocks the world, Obama says, BBC News, 2014). The incident was horrible, but it was not the first video where an ISIS terrorist beheaded someone, and it would not be the last. In May 2004, Abu Musab al-Zarqawi, the founder of ISIS and the leader of al-Qaeda in Iraq at that time, had executed Nick Berg, who was a U.S. citizen and published the execution video clip on an Islamic website (Siboni & Koren, 2015, p. 127). Steven Sotloff, who was a journalist and had a dual American-Israeli citizen, had abducted by ISIS militants in August 2013 in northern Syria, and then, the group released a beheading video exhibiting the execution of the Journalist in early September 2014 (Haaretz, U.S. journalist beheaded by ISIS was Israeli citizen, Foreign Ministry says, 2014). As can be seen from the examples, the video records were the most visual platforms that astounded the whole world against ISIS's brutal actions.

Magazines were a shift from an emphasis on power projection to more religious and ideological messages to the organization's followers, potential supporters, and militants. The usage of images along with texts in these magazines gave more intense messages to the target audience. *Dabiq* and *Rumiyah* were two substantive propaganda magazines of ISIS. *Dabiq* was an online magazine named by ISIS for the town of *Dabıq*, which believed a prophesied apocalyptic battle would occur, published in 15 issues between July 2014 and July 2016 in a number of different languages, including English (Welch, 2018, p. 3). *Rumiyah* also was an online magazine, named by the group for a reference to a hadith regarding the conquest of Rome by Muslims in the future, published in 13 issues between September 2016 and September 2017 in

different languages (including English) (Welch, 2018, p. 3). ISIS gave an unequivocal message to its enemies and the international community by entitling these magazines with the names of *Dabıq* town and Rome city that the group accepted these places as holy for their extremist ideology. Each issue of these magazines represented forty to seventy pages involving ten to seventeen articles that they divided into five categories: 1-Islamic teaching and justification, 2-stories of progress and heroism, 3-establishment of common enemies, 4- appeals to community, belonging, and meaning, 5-instructional and inspirational (Welch, 2018, p. 2). While *Dabiq* magazine articles predicated on the points of exceptional heroism, building community, and immigrating to the caliphate, *Rumiyah* magazine concentrated on the subjects of an emphasis on Islamic teaching and the encouragement of individuals (Welch, 2018, p. 3). According to the Washington Post, "hundreds of videographers, producers, producers and editors responsible for scripting, filming, cutting, and disseminating ISIS films, or laying out the monthly issue of *Dabiq*, formed a privileged, Professional class with status, salaries and living arrangements that were the envy of ordinary fighters" (Weiss & Hassan, 2016, pp. 211-212).

*Nasheeds* are chants that include Islamıc-religious messages and narratives. They were only for Muslim audiences, the organization's supporters, because of their religious nature. The main themes of the ISIS *nasheeds* were based heavily on clear and coherent messages that criticized the *ummah* for its weakness because it receded from true Islam; however, they were emphasizing there was hope for establishing the Islamic State and restoring Islam (Gråtrud, 2016, p. 32). The *nasheeds* could also include aggressive remarks to drive their followers to violent actions. For instance, the lyrics of a *nasheed* from Islamic State's *Ajnad* Media named "We have the Swords" shared by Aymenn Javad Al-Tamimi, who is a British specialist on the Iraqi and Syria Civil Wars, in its blog were that (Aymenn Jawad Al-Tamimi's Blog, 2015):

> The clashing of the spearheads is the melody of men,
> And in war there is might, and return of dignity.
> So arise for eternity, brother, come and
> shake off the path of stupid laziness
> And shake off the path of stupid laziness.

The organization also benefitted from news reports which were brief and informative, presenting power projection towards Western Media. The news reports were composed of pictures or infographics involving visual messages that contributed to the group's image war. After the Paris attacks, the jihadi group published an issue, with an infographic regarding the assaults in Paris, in its official weekly newsletter *Al-Naba* in which the group mention in one section that "the Paris raid has caused the creation of a state of instability in European countries which will have long-term effects," continued by addressing "the weakening of European cohesion, including demands to repeal the Schengen Agreement which permits free traveling in Europe without checkpoints" and "security measures will cost them tens of millions of dollars" (Hussain, 2016).

*3.2.2.1.2 Social media*

Pursuing a sophisticated and productive propaganda machine conducted by competent militants having substantial technical expertise, ISIS exhibited a functional posture at enlisting new militants from all around the world, with nearly 20 percent of those coming from Western nations (Macnair & Frank, 2017, p. 2). Through social media platforms, ISIS managed to gain an increasing number of foreign fighters (Greene, 2015, p. 50). Counting on social media platforms in its psychological warfare, ISIS tried to wage two essential functions through the usage of social and communication media apparatuses as by its propaganda machine: targeting the morale of the enemy elements and unifying its followers and supporters behind one goal under one leadership (Siboni & Koren, 2015, p. 138). ISIS members and supporters used Twitter and other social media platforms such as Facebook and YouTube to recruit new members by enticing them with heroic stories, and built up a modality based upon intimidation and creating fear in the hearts and minds. The followers, supporters, and sympathizers of the group actively participated in Twitter. They wielded Twitter as an ISIS megaphone, rendered service to the organization, and promoted its ISIS brand.

According to a study that analyses defining and describing the population of ISIS supporters on Twitter (Berger & Morgan, 2015);

- The group used at least 46.000 Twitter accounts from December 2014 (to March 2015 when the study was released),
- Nearly one in five ISIS supporters ran their accounts in the English language when using Twitter, and three-quarters of them ran by the Arabic language,
- ISIS-supporting accounts had about 1.000 followers each that substantially were higher than a standard Twitter user and more active than non-supporters.

Venomous preachers had strived to provoke large numbers of followers on YouTube; Sheikh Mohammad al-Zughbi, a popular vlogger in Egypt, called to God to protect Egypt from Shiites, Jews, and Crusaders in his vlog, and in another vlog entitled "Oh Syria, the victory is coming," the vlogger said that President Bashar Assad of Syria sought help from these Persians, the Shia, the traitors, the Shia criminals (Cockburn, 2014, p. 131).

Showing the skill of ISIS to produce flamboyant propaganda and military films, "Clanging of the Sword" was the most typical example of jihadi pornography, which was released two weeks before the fall of Mosul and distributed on social media platforms such as YouTube, Twitter, and Facebook and websites such as archive.org and justpaste.it (Weiss & Hassan, 2016, p. 212). The film that ISIS boasted itself involved so many brutal actions, bloody scenes, and violence. Through the film, ISIS made its ill-minded propaganda and intended to agitate its supporters by unfolding their deviant mentality. Besides, the film displayed the group's apparent omnipresence and undercover tradecraft in reaching its enemies (Weiss & Hassan, 2016, p. 213).

The usage effectively of social media apparatuses and traditional media tools by the Islamic State as its propaganda tools generated fear among the international community and caused ISIS to drum up increasingly among the group's followers/supporters. Indeed, the trademark of ISIS's success was utilizing social media platforms as part of the nature of the group's psychological warfare in its fighting strategy. By various media means, the Islamic State obtained the opportunity of spreading its teachings, dictating its political and religious legitimacy, creating fear in the hearts and minds, enlisting new members, appealing ones inclining extremist thoughts, communicating with people of the world. Observed the surging of ISIS propaganda videos on social media platforms and the rise of abhorrent activities of the

group in the Middle East and Western countries, the United States had tried to prevent the group's social media activities by taking countermeasures such as deletion of their online content, suspension of social media accounts, hacking the group's websites (Shehabat & Mitew, 2018, p. 81). However, the Islamic State adopted its countermeasures and moved its propaganda network to other encrypted communication channels such as Telegram, Signal, and WhatsApp, as well as anonymous sharing portals such as Justpaste.it, Sendvid.com, and Dump.to (Shehabat & Mitew, 2018, p. 81). These platforms enabled ISIS to continue its social media activities without suffering from efforts that aimed to degrade its media network and sustain its global information operations even if the coordinated efforts at obscuring and filtering (Shehabat & Mitew, 2018, p. 98).

#### *3.2.2.2 Image war of ISIS*

As part of the fighting strategy, ISIS's usage of information served the purpose of strengthening the group's image war, which forged public awareness and support among Muslims, managed media platforms, and enlisted media operatives as its militants (Yarchi, 2019, p. 63). ISIS constituted such an image thanks to its effective media strategy by exploiting modern media tools as well as traditional ones that it became a brand in psychological warfare. Al-Hayat Media Center, which was the Islamic State's primary Western-oriented media outlet, allocated a distinguished image for ISIS by generating videos with assorted themes; seven predominant themes of that were 1-production quality and video styles, 2-comradery, brotherhood, inclusivity, 3-depiction of violence, 4-strength and victory, 5-the crimes of enemies, 6-calls for recruitment, 7-existential and spiritual fulfillment (Macnair & Frank, 2017, pp. 3-15). Thus, the terrorist group achieved to set a brand that would depict its image of war in its psychological warfare.

#### *3.2.2.3 Strategic communication and ISIS*

The psychological warfare of ISIS was predicated on strategic communication and propaganda actions rather than disinformation and misinformation campaigns which is the intentional or non-intentionally dissemination of false information. To reach a broad audience, ISIS had reached such a great level in its information warfare by using strategic communication that it left behind other *Salafi*-jihadist organizations such as Al-Qaeda and Al-Shabab (Yarchi, 2019, p. 56). ISIS adopted an image war being a prominent of its activities and built its strategic narrative on three elements; 1- a positive narrative on ISIS's achievements, 2- counter-speech against its critics and enemies, 3- weaponized propaganda (Yarchi, 2019, p. 56).

The group drove a media strategy in which it deliberately addressed salient themes such as fighting, Islamic religious messages, violence, and power protection and purposeful contents such as Islamic teachings, heroism, determining common enemies, and spreading the extremist ideology. With these themes and contents, the group aimed to influence the behaviors and perceptions of the target population and create a climate of fear among the international community. In this way, it tried to control and direct opinions, thoughts, beliefs, emotions of both its followers\supporters and its adversaries.

ISIS had definite goals and objectives aimed at managing an effective communication strategy, such as recruiting new members/militants for the organization, placing its ideas\thoughts into the minds of Muslim youths, threatening its adversaries, and spreading fear in the hearts and minds of them. Two main views pointed out the communication goals and objectives of ISIS and its corresponding message strategies and tactics of it. 1- to intimidate opponents with psychological warfare, 2- to build political and religious legitimacy and credibility as a utopian caliphate (Royo-Vela & McBee, 2020, p. 5). In this manner, the group endeavored to reach its ultimate objective, which was to establish an Islamic caliphate on the basis of *Salafi* ideology and expand its occupied territories to Muslim countries to unify under the supreme caliph and rule them by Sharia Law.

To illustrate how ISIS handled the five tenets necessary to create effective strategic communication that will help organizations achieve goals and objectives:

→ Intentional Message Design: ISIS disseminated its intentional messages relying on discursive and textual content and practices. The group followed a media strategy hinged on both traditional and modern media methods with salient violence, extremist, brutal content. In this way, it purposed to influence, direct and change of behaviors and thoughts of the target audience.

→ Correct Platforms: Communication environments ISIS benefitted were mainly traditional media apparatuses such as magazines, audio statements, videos, news reports and, modern media tools like internet platforms, mainly social media platforms.

→ Calculated Timing: ISIS haphazardly released its both traditional and modern media tools without any strategic timing. However, ISIS had a command and control structure that tightly adhered to its communication content, and the media products were not being uploaded and released to the internet at random (Schneider, 2015, p. 12).

→ Audience Selection and Analysis: ISIS had three target groups that showed interest in ISIS's intentional message and responded to the message; 1- supporters consisting of potential recruitments and active fighters\members, 2- the local populace, which was people living in the lands under the rule of ISIS in Iraq and Syria, and 3- enemies comprising local, regional and international entities like states, governments, other jihadist terrorist groups (Royo-Vela & McBee, 2020, p. 5).

→ Desired Impact: For ISIS, the desired impact was the responses ISIS received from the international community and its supporters. How much ISIS achieved to create fear and anxiety among the community and how much ISIS got support from its followers and recruited new members to its organization, intentional messages released by ISIS via various media tools was successful and effective to that extent.

### 3.2.3 Cyberwarfare of ISIS

ISIS was a leading NSAA in performing cyber terrorism and cyber vandalism when considering its cyber operations. After land, air, and sea, cyberspace was another

combat area for ISIS. ISIS used to good advantage of information technologies on the ground of new terrorism concept. The terrorist organization took a different and effective track because it had unique characteristics and blended conventional and non-conventional warfare methods in its war. ISIS mostly managed its propaganda activities, recruitments, intimidation, and provocation campaigns through cyberspace as a hybrid-warfare method. Compared to other terrorist entities, ISIS used cyberspace more intensely and talentedly at a certain level. ISIS had formed a cyber-army to convey its actions in cyberspace in addition to its traditional acts of terrorism.

The most crucial power of ISIS was its ability to influence human minds by conducting psychological operations. Although the history of psychological warfare dates back to very early times, the advantage of ISIS was an ever-growing and developing technology. It performed its psychological warfare by benefiting from this technology to a considerable extent. Internet platforms, products of this technology had vital importance for the group to maintain its existence. Besides, the cyber warfare of ISIS was in integrity with its psychological warfare strategy. As ISIS conducted its tactical, optional, and strategic operations regarding psychological warfare, cyberspace was a domain utilized by the organization. The omnipotent pattern of the cyber domain and its use as a weapon by ISIS created appreciable concerns in the international community.

#### *3.2.3.1 Cyber strategy of ISIS*

An operation in the cyber domain is more lucrative and riskless than a conventional operation in terms of cost and expenses. Executing an ordinary terrorist operation necessitates a set of preparation and planning processes with high expenses and hefty prices. Being aware of this, ISIS took advantage of the cyber domain for several purposes: recruitment, provocation, intimidation, and the spread of its ideology.

ISIS pursued a quite brutal, fundamentalist, barbarous way in order to actualize its objectives. As part of its overall strategy, the cyber strategy of the group aimed to carry out cyber-attacks, generate fear and anxiety, perplex human minds, conduct all

sorts of propaganda, manipulation, and disinformation campaigns upon individuals, populations, and governments. The cyber strategy of ISIS focused on mainly four categories: intimidation strategy, provocation strategy, outbidding strategy (Smith, 2017, p. 56), and recruitment strategy.

#### *3.2.3.1.1 Recruitment strategy*

This strategy served ISIS's goal of recruiting new members by identifying, attracting, and inducing sympathizers through cyberspace. ISIS also enlisted hackers from all over the world. Some were virtual accomplices from a distance cooperating with ISIS to sustain its recruitment and propaganda actions; others were supporters who immigrated to Syria to maintain internet access in ISIS territories (Graham-Harrison, 2015).

ISIS had heavily leveraged virtual space for recruiting. The group spread its ideology via social media, which was one of the most convenient internet platforms for recruits. For this reason, the group activated its cyber fighters to detect potential recruits by hacking users' social media accounts so that they could find out jihadi-inclined supporters and induce them to participate in the group. In addition, they broadened the scope of their propaganda activities by disseminating their ideology through hacked accounts as much as possible. With their selective qualities, social media platforms that offer users to find like-minded individuals enabled these jihadi-inclined individuals to contact each other and create ensembles and groups among them. Besides, ISIS cyber fighters could access users' personal information such as name, place of birth, phone numbers, addresses, and employee records via these platforms.

The organization manipulated computer games in addition to other information systems-based platforms such as Twitter, Facebook, Telegram, and YouTube to communicate and recruit new members. To avoid government surveillance, ISIS followers relayed messages among the members and sympathizers by using Sony's PlayStation 4, which was more sophisticated to monitor than other encrypted messaging apps like WhatsApp (Neagle & Neagle, 2015). However, how exactly ISIS

used Sony's PlayStation 4 for communication and which ways pursued by the organization were not unequivocal.

ISIS also benefitted from computer games to set out its extreme ideology and method on internet platforms. To give an example pertaining to the management of computer games by the group to exhibit its ideology, the organization improved a game called "Jihad Simulator," in which players hijacked military vehicles and blew them up, carried out drive-by shootings of American police cars, and shot up randomly everywhere within sight regardless of whether it is school or office park (Shamah, 2014). In that way, the group strived to influence human minds, more in particular intended for youth minds, to enlist new members and diffuse its extremist jihadi ideology into their minds.

*3.2.3.1.2 Intimidation strategy*

As a part of its psychological fighting strategy, ISIS used the cyber domain to intimidate the international community and its enemies by carrying out psychological operations. The group led such a psychological warfare campaign that a part of this warfare campaign was on the pillar of the cyber domain. Cyberspace submitted the group an unprecedented opportunity to implant a brutal image of a terror state into the minds of people around the world in parallel with its psychological warfare.

ISIS-affiliated hackers hacked about nineteen thousand French Websites in the wake of the attacks on the Charlie Hebdo office on January 7, 2015; such websites as French businesses, religious groups, universities, municipalities that substituted these websites the legends displaying pro-ISIS messages and black ISIS flags and "Death to France" (Akbar, 2015). After such an incident as the Charlie Hebdo office attack that stunned the whole world, hacking of French websites and placing its messages there by the group was an example of the group's intimidation strategy.

*3.2.3.1.3 Provocation strategy*

In order to provoke its enemies, ISIS attached importance to the cyber domain and aimed to drag them into anxiety by performing cyber-attacks on their computer systems. In line with its provocation strategy, its jihadi hackers tried to attack some notable government infrastructures. Operated cyber actions against governments by ISIS were one of the components of the cyber warfare that ISIS runs against its enemies.

ISIS cyber fighters had attempted to hack American electrical power companies, but they were not accomplished, and the attack failed to inflict irreparable damage because of their immature cyber capacity. So, this aroused concern in the Federal Bureau of Investigation (FBI) regarding the probability was that ISIS and its supporters would possess malicious software that could sneak into computers and destroy power companies that, would result in a damaging flow of energy to homes and businesses (Pagliery, 2015).

Being an enterprise software company, PKWare predicted that ISIS would target American and Western businesses due to its augmenting cyber capability, and ISIS would execute a major cyber-attack on a U.S. presidential campaign and assaults on U.S. electric grids (Taschler, 2016). However, these were predictions for the distant future, and there was no critical indication that the group would become an advanced cyber power that would compete with states in the near future. The group was striving to perform cyber-attacks on government infrastructures but failed to inflict irreparable damage.

ISIS-affiliated hackers claimed that they had essential cyber capabilities to strike computer systems in the U.S. and Europe, and accordingly, thanks to skilled hackers that would able to attack worldwide computer systems, ISIS cyber armies carried out some cyber-attacks on the social media accounts belonging to the United States Central Command (CENTCOM) and released a propaganda video warning the West: “What you have seen is just a preface of the future. We are able until this moment to hack the website of the American leadership and the website of the Australian airport and many other websites” (Paganini, ISIS – Cyber Caliphate hackers are threatening Electronic War, 2015). In addition, ISIS proponents hacked into the Twitter and YouTube

accounts of CENTCOM forces in the Middle East and South Asia. They replaced the Twitter account of CENTCOM with a masked image of a militant and the inscription "CyberCaliphate" and "I love you Isis," and simultaneously inserted two pro-ISIS videos into the YouTube accounts of the CENTCOM while Barack Obama was giving a speech in Washington regarding cyber security (Ackerman, US Central Command Twitter account hacked to read 'I love you Isis', 2015).

ISIS was the first extremist group with a credible offensive cyber capability to perform any cyber-attack against a government infrastructure (Paganini, Mikko Hyppönen warns the ISIS has a credible offensive cyber capability, 2015). Even though cyber-attacks against government infrastructures performed by ISIS hackers were not successful or long time impact on these infrastructures, they achieved to create concern for future attacks. Notwithstanding, the group has not yet adequately performed more multifaceted and high-level cyber assaults; It is possible that the cyber ability of the group would increase day by day due to its recognition of the efficiency of cyberspace.

The organization developed an application for mobile devices called "Dawn of Glad Tidings" that allowed ISIS to take temporary control of the users' Twitter accounts and publish messages in their name (Hoffman & Schweitzer, 2015, p. 74). The taking and managing of social media accounts of ordinary users by ISIS on behalf of themselves pointed out how ISIS operatives exploited their social media accounts and capitalized on other users' accounts to consolidate their propaganda activities on social platforms.

#### *3.2.3.1.4 Outbidding strategy*

The outbidding strategy is a mechanism that turns a passive supporter, who is an undecided individual, into an active member by showing examples that allegedly represent the interests of the individual. (Smith, 2017, p. 56). Within the context of outbidding strategy, ISIS induced foreign fighters from all over the world to participate themselves and turned them into lone-wolf terrorists who had the ability to carry out independent assaults at any time and any place.

Moreover, the organization mobilized lone wolves from all parts of the world to organize terrorist and violent actions through the cyber domain. A Lone wolf is an actor who acts independently and commits terrorist activities alone that do not belong to any terrorist organization. Lone wolves of ISIS were not de facto formal members of the group, but they were sympathizers of the group. They were inspired by ISIS and perpetrated terror actions in the name of ISIS. These actors swiftly came into action when called. 2015 Paris attacks were one of the examples of ISIS's lone-wolf terrorist strategy.

As a part of the 2015 Paris attacks, Moroccan Ayoub El Khazzani was charged with opening fire on passengers at the Thalys high-speed train en route to Paris on August 21, 2015 (Hankiss, Agnes; Counterterrorism Department of the National Securi;, 2018, p. 56). At first, Khazzani had no apparent connection to the Jihadi terrorist organization, but then, it revealed that he had a remote connection with Abdelhamid Abaaoud, who was o ISIS militant and a key figure in the Paris and Brussels attacks (Hankiss, Agnes; Counterterrorism Department of the National Securi;, p. 56).

#### *3.2.3.2 Cyber Caliphate*

United Cyber Caliphate (UCC) or the Islamic State Hacking Division (ISHD), forming from some of ISIS cyber army subgroups such as Ghost Caliphate Section, the Sons Caliphate Army, the Caliphate Cyber Army, and the Kalashnikov E-Security to promote their hacker capabilities, carried out cyber operations, recruited new followers, and offered security advice regarding actions in cyberspace (Liang, 2017, p. 16). The hacking group organized cyber-attacks against different countries such as the United States, France, Australia, and the United Kingdom on behalf of the Islamic state. UCC released a video message that threatened the U.S. and President Trump and published a kill list of 8.786 names and addresses intending to direct ISIS followers to kill them wherever they come across (Liang, 2017). In this way, they both tried to generate a climate of fear, and on the other hand, they made the ones on the kill list for lone wolves as a target.

The cyber army of ISIS had talented hackers that most of them recruited by the group from Western countries. Ardit Ferizi, a Kosovo citizen and believed to be the leader of a Kosovo internet hacking group known as Kosovo Hacker's Security, was charged with providing material support to ISIS and committing hacking and identity theft offenses, and distributing personally identifiable information of U.S. service members and federal employees to ISIS (The United States Department of Justice, Office of Public Affairs, 2015). Besides, as a part of ISIS's Cyber Caliphate and a British hacker Junaid Hussain, also known as Abu Hussain al-Britani, was a prominent figure of the organization that he had seized on the passwords of the U.S. Central Command's Twitter and YouTube accounts and granted them to ISIS possession (Ackerman, MacAskillin, & Ross, Junaid Hussain: British hacker for Isis believed killed in US air strike, 2018). Namely, not also the organization did recruit members from western countries for fighting, but it recruited skillful hackers from these countries to carry out cyber-attacks or obtain information about target individuals or organizations.

#### *3.2.3.3 Dynamics of ISIS'S cyberwarfare*

ISIS-affiliated hackers endeavored to execute cyber-attacks against various government infrastructures, their target figures, and entities, such as politicians, bureaucrats, governments, businesses, from distinct countries at different times; target enemies were usually the assets of the governments of Western countries. The cyber-attacks performed by these hackers were attacks with short-term effects that did not cause irreparable damages. Some examples of these attacks are listed below.

- UCC hacked the websites of more than twenty small Australian small businesses, including wheel and tyre retailers and a Mexican food catering company, on April 15, 2016, by leaving a picture written: "In the name of Allah, we are United Cyber Caliphate. Obey Islamic State. Your system is fail. Islamic State #rules, (Ockenden & Sveen, 2016)." In the wake of hacked

Australian businesses, the group warned Australia of the probability of the subsequent attacks.

- In April 2015, the Hobart International Airport website, a small airport in Tasmania, Australia, came under a cyber-attack held by Islamic State hackers; the hackers lodged a threatening message appended a black-and-white picture of an ISIS member including insulting the United States and Israel (The Jerusalem Post, 2015).
- In early August 2015, a hacking group was associated with Islamic State posted a list of names and contacts belonging to one thousand four hundred American government and military personnel that included their phone numbers, locations, and passwords (McConnell & Todd, 2015). By sharing the list, the group intended to point these staff as targets to the group sympathizers and urge them to attack listed personnel.
- According to the Government Communications Headquarters (GCHQ), an intelligence and security organization of the United Kingdom, ISIS hackers breached the email accounts of some of David Cameron's senior ministers, including the Home Secretary Theresa May, to collect information related to the key ministers of the United Kingdom in September 2015 (Paganini, ISIS hackers violated top secret British Government emails: Security Affairs, 2015).

### 3.2.4. Economic warfare of ISIS

As a terrorist organization, the Islamic State had derived its incomes from mostly economic activities on the territories under its rule. In addition to this, the organization captured a considerable amount of revenue from donations granted by foreign countries and made money from human trafficking. The income that the organization acquired had financed the organization's economic, social, political, and military activities.

#### *3.2.4.1 Revenues*

Being one of the wealthiest terrorist organizations, ISIS earned hundreds of millions of dollars a year by grabbing almost every aspect of the economic revenues of its occupied territories, from trade, agriculture, remittances to salaries that the governments paid their fighters (Solomon & Jones, Isis Inc: Loot and taxes keep jihadi economy churning; Financial Times, 2015). As ISIS enlarged its lands, it also caught the chance to have additional income by capturing new oil fields and collecting taxes, fees, fines from the people living in these territories. ISIS raised its majority of revenue by smuggling oil and products from the Iraqi and Syrian oil sectors, by extorting assets in those sectors, through extortion and taxation of the local economy in the areas it controlled, by looting war spoils (such as the region's rare and worthful antiquities), by selling stolen and looted goods in the black market, by receiving money from external donors as well as by collecting money through kidnapping and ransoms (Johnston, Countering ISIL's Financing, 2014, pp. 2-4).

The chart Figure 3 (Heißner, Neumann, Holland-McCowan, & Basra, 2017, p. 8)) illustrates that ISIS generated income from four main revenue items in 2014, 2015, and 2016 (by neglecting other revenues); taxes and fees, oil sales and smuggling, kidnapping and ransom, and looting and confiscations. The group earned a total of 1890$ million just from these primary four items in 2014. This revenue had decreased to 1700$ million in 2015, and it became 870$ million by further reducing in 2016 as a result of the US air campaign aimed at bombing oil and gas facilities operated by the Islamic State.

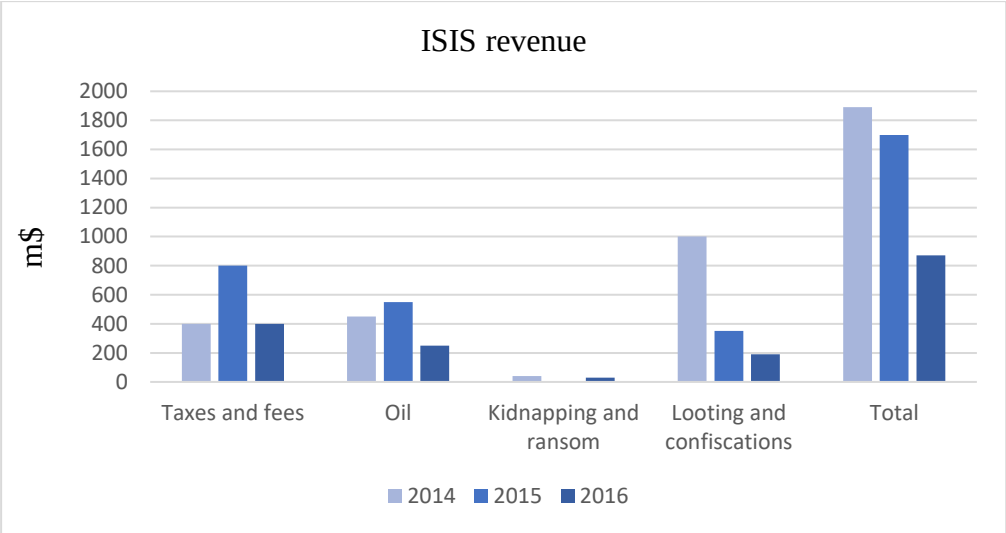


Figure 3: ISIS Revenue, Source ICSR. Note: 2015 kidnapping figure is unclear. (Other revenue items are not calculated).

As to ISIS's expenses, the group spent its revenues mainly on four goals; 1- sustain its expansion in Iraq and Levant (a vast area of Syria, Lebanon, Israel, the West Bank, and Gaza), 2- expand its influence in other strategic parts of the Muslim lands, 3- fund plans for attacks in North America, Western Europe or elsewhere, 4- fund its members and finance its current territories and its Sharia-based state that it intended to establish (Johnston, Countering ISIL's Financing, 2014, p. 3).

*3.2.4.1.1 Taxes, Fees, and Extortion*

ISIS collected ordinary state taxes, extortions, and religious taxes involving fines and penalties for not being bound up with its extremist social and political law from the people in its territories (Blannin, 2017, p. 17). The group applied assorted tax tariffs against different income groups and revenue items, levied a 10 percent income tax, 10-15 percent tax on business revenues, 2 percent value additional tax, and laid taxes on smuggling drugs and weapons, road and customs for vehicle crossing, also received departure taxes of up to 1.000 dollars from the people wanting to leave ISIS lands (Blannin, 2017).

*3.2.4.1.2 Looting, Confiscations*

ISIS-affiliated extremists took $101 million and $727.6 million from banks in its controlled areas in the wake of creating the so-called caliphate in July 2014; thereby, they plundered a total of more than $800 million from Iraqi banks (Moore, 2017). This brought enormous wealth to the terrorist organization.

As of autumn of 2014, ISIS began to make excavation contracts and hired their own archeologists, digging teams, and machinery to pump money into its coffer from looting activities, which would be lucrative enough for the group, and this coincided with the US-led coalition's airstrikes, which caused in reducing ISIS income streams such as oil, crops from occupied areas (Shabi, 2015). Earned nearly 36$ million from the sales of antiquities in 2014, the group managed more than 4500 archeological sites in Iraq and took control of museums, private collections, and archaeological sites that provided the group an extending supply of precious art and historical artifacts in 2015 (Blannin, 2017, p. 16).

*3.2.4.1.3 Natural Resources*

Oil had been one of the vital revenue items for ISIS to fund its whole organization circle and sustain its sophisticated warfare strategies. ISIS took over 60 percent of Syria's oil assets, including the Al Omar, Tanak, and Shadadi oil fields, enabling the Jihadi group to become a hybrid organization (Pape & Morell, 2015). In order to sell its oil, ISIS had established a highly organized system in which Syrian and Iraqi independent traders straightly went to the oil fields with their trucks to purchase crude oil, but this had caused these traders to wait for weeks in traffic jams that spread for miles outside the oilfields (Solomon, Kwong, & Bernard, Syria oil map: the journey of a barrel of Isis oil; Financial Times, 2016).

Controlling most of Syria's oil fields, ISIS had procured between 34.000 to 40 barrels a day in Deir Ezzor, which was the group's primary oil-producing region, in Syria's eastern province until at the end of October 2015, when the US coalition launched airstrikes on ISIS oil infrastructure, and afterward, Russian attacks followed

this (Solomon, Kwong, & Bernard, 2016). The oil prices differentiated between $25 a barrel and $45 a barrel depending on oil's qualities in fields, and ISIS earned estimated about $1.5 million a day before the US coalition And Russian airstrikes (Solomon, Kwong, & Bernard, 2016).

Despite the efforts of the US coalition and Russia, the group had a sprawling business almost like a state oil company that was enlarging in size and expertise, and the ISIS oil company vigorously enrolled skilled employees from engineers, trainers to managers (Solomon, Chazan, & Jones, Isis Inc: how oil fuels the jihadi terrorists: Financial Times, 2015). Besides, after passing through northern Iraq and conquering Mosul, ISIS seized Ajil and Allas fields in northeastern Kirkuk province in Iraq and sent its militants to safeguard the oil fields and employed engineers in there (Solomon, Chazan, & Jones, 2015).

*3.2.4.1.4 Kidnapping Ransoms*

Kidnapping for ransom was one of the most substantial revenue sources for terrorist organizations. ISIS earned income by kidnapping some foreign citizens, journalists, wealthy individuals for ransom. The group took at least 20$ million in ransom in 2014 due to releasing captured journalists and hostages from European countries and earned several multi-million dollar payments in this way (U.S. Department of The Treasury, 2014).

*3.2.4.1.5 Other Sources of Income*

ISIS took in its coffer an amount of money through other sources of income such as donations, agriculture, mineral deposit reserves, and dams. The jihadi group also received some funding from wealthy private regional donors, but this funding was minimal compared to its other revenues (FATF, 2015, p. 18). Additionally, the US Department of the Treasury ratified that the Islamic state took 2$ million donations from the Gulf on September 24, 2014 (FATF, 2015). Moreover, the group controlled over notable swathes of the Iraqi farmland, collected portions of wheat and barley

crops from farmers as Zakat, and it leased back to the farmers the agricultural machinery that it had previously confiscated from the farms (FATF, 2015, p. 15). Besides, the group accepted that it made a vast amount of income from human trafficking; the estimated price of human smuggling in Libya was 323$ million in 2014, while from Syria to Turkey could increase over 8.000$ for an individual (Besenyő, 2016, pp. 16-17).

#### *3.2.4.2 Dynamics of Economy of ISIS*

As mentioned in chapter two, economic warfare has primarily three purposes; economic, military, and political. In terms of military-purposed economic warfare, ISIS could run such warfare to obtain money for purchasing weapons to use them on the battlefields in war times. As for political-purposed economic warfare, ISIS was not in a position to implement any economic pressure on states, which are legal entities, to bring them to their knees. Moreover, pursuing a political purposed economic warfare was out of the question for ISIS. ISIS was an illegal entity for being a terrorist organization, and it could not wage for the acquisition of political advantages such as the desire for respectability and status, the takeover of another country by economic means, making economic alliances. Besides, conducting a kind of economic warfare based on economic-purposed was not in the realm of possibility for the terrorist group. Guaranteeing sources of supply, guaranteeing markets, improving the terms of trade, denial, and economic takeover were economic purposes of waging economic warfare, and ISIS was not in a position to perform these purposes due to its illegal nature.

The truth of the matter was that ISIS was a terrorist organization that was destitute of integration of the legitimate economic and financial systems because of its illegal nature. Therefore, ISIS did not have the power and opportunity to use the main tools of economic warfare such as embargoes, boycotts, blockades, sanctions, or economic strikes against its adversaries.

Captured more than 90.000 km2 of territory by early 2015, ISIS had reached its peak with 104.000 km2 (16.7 percent of Iraq and Syria) as of the first half of 2015 (Johnston, Alami, Clarke, & Shatz, 2019, p. 44). This large territory was so crucial and

vital for a terrorist organization like ISIS, which derived its supply chain and most of the revenues from territories it governed. Natural resources, kidnapping for ransom, lootings, and taxes were most of the incomes of ISIS had on its territories. Besides pretending like a state while controlling the territories it occupied, ISIS raised its revenues by imposing tariffs on imports at a rate of 2.5 percent, levying taxes on the population under its governing, enforcing licensing fees on businesses in the amount of between 2.500$ and 5.000$ (Mansour & Al-Hashimi, 2017). The preservation of these revenues depended on guaranteeing the soils the group governed.

On November 15-16, 2015, leaders of the group of 20 called for cooperation and coordination to halt funding channels to terrorist organizations, including exchanging information and freezing their assets; however, this was not effective for ISIS because the group procured funds in its own territory and spent in there (Swanson, 2015). However, the revenues of the Islamic State had begun to decrease because of the aggressive countermeasures consisting of an air campaign implemented by the US that targeted the group's main revenue items as of late 2015; these countermeasures included (Johnston, et al., p. 49):

- bombing oil and gas assets and supply chain of the group,
- reducing tax revenues by making them lose their land,
- bombing bulk cash facilities of the organization,
- preventing its access to the formal financial system,
- killing financial leadership.

After this stage, as ISIS lost its territories as a result of the US air campaign, the incomes of the group began to decrease gradually. Although the incomes of ISIS had fallen markedly due to the coalition airstrikes, oil smuggling to Jordan and the other regions of Syria and Iraq was still an essential source of income for the group (Weiss & Hassan, 2016, p. 263). In order to compensate for the reduction in its incomes, ISIS had transferred its some liquid assets into Jordan banks to speculate in the stock market and then took back the profits to send the regions of Iraq the group controlled (European Parliament, Directorate-Gen.l for External Polic. of the Union, Cousseran, & Levallois, 2017, p. 16).

In addition, ISIS took various countermeasures to avoid its revenues from being eroded, such as (Gerges, 2016, p. 268):

- Reduced fighter's salaries from 400$ a month to nearly 300$,
- Imposed additional taxes and fines on the inhabitants,
- Reduced aid programs,
- Prolonged electricity cuts.

Indeed, ISIS had built a multidimensional economy that was not contingent upon one source; as the coalition airstrikes crippled the revenues from natural sources, the group tried to equilibrate its incomes by applying pressure on the population under the Islamic state to collect more taxes and extortions (Gerges, 2016, pp. 268-269).

### 3.2.5. Electronic Warfare of ISIS

ISIS turned into a conventional power with the potential for simultaneous conflict, regular units and irregular combat power, armored and fire support potential, air defense power, shallow water operation, and the ability to use the unmanned aerial vehicles and its weapon-ammunition and equipment capability were higher levels than known (Ağar, 2015, p. 385). However, any notable information about ISIS having advanced electronic weapons did not exist in the literature. The electronic tools of ISIS were limited to communication tools, unmanned aerial vehicles (UAV) s/drones, and a missile. Besides, there was some knowledge regarding the group that had Chemical, Biological, Radiological, and Nuclear (CBRN) Weapons. But, in order for ISIS to carry out all-out electronic warfare, it had to have a much more extensive electronic capacity.

Cyberspace and communication technologies were some electronic tools used by ISIS. The jihadi group had tried to exploit cyberspace by performing cyber-attacks against different countries like the United States, France, and their governments, politicians, bureaucrats, but they did not achieve any significant success in this way. ISIS utilized communication technologies to disseminate propaganda activities as part

of its psychological warfare. However, this was not adequate for the group to wage electronic war.

The Islamic State employed UAVs with the intention of several missions such as reconnaissance and surveillance, filming of its operations, collecting imagery intelligence, practicing strikes against enemy targets. The terrorist organization consigned a wide variety of drones to conflictual areas, including grenade-dropping drones, quadcopters, kamikaze bombers, flying decoys, on these missions (Watson, 2017). ISIS benefitted from several kinds of drones, but the group mainly preferred small quadcopters because of that they were able to rig to drop small munitions with the approximate explosive power of a small hand grenade (Sisk, 2017). ISIS militants dispatched a modified DJI Phantom FC40 quadcopter for the purpose of reconnaissance mission prior to an assault against the Syrian army base in northern Syria on August 23, 2014, which was evidence that the group benefitted from drones with the intent of reconnaissance and surveillance (Lasconjarias & Maged, 2019, p. 9). Drones have a feature that they can gather, analyze information, and record activities as it occurs on the ground (Sims, 2018, p. 103). Obtained data from these records had provided an opportunity for ISIS to fix this data into its well-organized terror network and consolidate its intelligence apparatus with this data to increase the group's coordination. United States Special Operations Command (USSOCOM or SOCOM) commander said that being an adaptive enemy, ISIS retained tactical superiority in the airspace via commercially available drones and fuel-expedient systems, which was a daunting problem in 2016 for the US because the response against ISIS drones was small arms fire (Larter, 2017). The dispatching of drones to conflictual zones, the beneficial usage of them by ISIS, and creating restlessness for US commanders was evidence that the group had a considerable drone strategy.

As a prosperous terrorist organization, the Islamic State had the purchasing power for a set of electronic weapons such as missiles, anti-aircraft weapons, reconnaissance, and surveillance systems. The purchase of these weapons required a step-by-step process involving international conventions and agreements between legitimate countries and organizations. However, because of its illegal entity, ISIS was not involved in purchasing any electronic or other weapons from these legitimate

actors. The only way to procure these weapons for the organization was to capture them.

ISIS made an appearance in Raqqa, Syria, on July 2, 2014, with a Scud missile, a long-range ballistic missile, and has complex systems carrying weapons systems with radar and nuclear head (Cumhuriyet, 2014). However, US officials said that the Scud missile was of Syrian origin, under the UN supervision Iraq destroyed its Scud missiles more than a decade ago, and to be able to launch this missile, ISIS would need maintenance personnel, fuel, a refueling vehicle, and skilled operators, in that the missile looked like a short-range Scud used by Iraq in the Gulf war and by the Syrian government in the civil war (NBC News, 2014). For this reason, having such missiles which did not benefit in war zones had not contributed to the terrorist organization's electronic tool capacity.

ISIS captured WMD technology and some components at a low level. A Syrian rebel group had found a laptop belonging to the Islamic State, which included a 19-page document on developing biological weapons and weaponizing the bubonic plague from infected animals and turning it into a weapon (Doornbos & Moussa, 2014). Also, the documents proposed that the owner of the laptop had tried to teach himself about the use of biological weaponry regarding preparation for an attack would shock the world (Doornbos & Moussa, 2014). Furthermore, ISIS-led Sunni rebels had taken control of a deserted factory, the Muthanna complex in the northwest of Baghdad, which housed remnants of rockets filled with sarin and other deadly nerve agents; however, according to the UN and US, the munitions were fruitless to use for chemical arms (BBC News, 2014). Besides, the Islamic insurgents seized nuclear materials from Mosul University in 2014; the university had had approximately 40 kilograms of uranium compounds (Burnett, 2014). However, the group had many obstacles to developing this low-enriched uranium into a nuclear device, but the group could make a dirty bomb by using these materials (Eweiss, 2016, p. 3). Developing a nuclear weapon required many obstacles for ISIS because it had to build an improvised nuclear device or acquire an assembled nuclear weapon even if the group had well-qualified technicians (Eweiss, 2016). Notwithstanding that the group seized some materials related to CBRN weapons, the organization did not afford to manufacture nuclear or CBRN weapons.

A document reached by Zaman al-Wasl, a Syrian news website, purported, without going into detail, that ISIS had some Electronic Warfare projects, including remote control car bombs, an electronically timed Grad missile, a rocket to explode missile in the air and test it as an anti-aircraft weapon, an automatic steering system for artillery weapons (Zaman Al Wasl, 2017). The document mattered in recognition of showing that the terrorist group had tried to develop electronic weapons and had somehow technically equipped personnel.

# 4. THE INFORMATION WARFARE CAPABILITY OF ISIS: THE ANSWERING OF THE RESEARCH SUB-QUESTIONS

The aim of the study was to illustrate the information warfare capability of an NSAA over a case and offer a perspective regarding how an NSAA uses it. In line with this purpose, the study submitted a theoretical framework concerning information warfare and its main five types in the second chapter and then, in the third chapter, investigated the subject of ISIS, which was the case of the study as NSAA on the basis of information warfare. Within this context, this chapter of the study allocated findings derived from the information in the third chapter and tried to evaluate research sub-questions.

## 4.1 Information Warfare Capability of ISIS

In this section, the study concentrated on the types of information warfare of ISIS in line with the information given in the previous section and tried to comprehend command and control, psychological warfare, cyber warfare, economic warfare, and electronic warfare capability of ISIS. The study sought to make inferences from the previous sections and formed the research findings.

### 4.1.1 Command and Control Capability of ISIS

Given that command and control ability hinge on nine command and control warfare prerequisites, the study examined these prerequisites one by one. Analyzing these prerequisites - knowledge and experience, operational picture, trust, information flow, situational awareness, objectives, feedback, flexibility, and decision making- of the command-and-control ability of ISIS gave information about the extent to which the group was successful in command-and-control warfare.

As a result of examining the command-and-control ability prerequisites one by one, the following results emerged. The first prerequisite (knowledge and experience)

of the command-and-control ability of ISIS informed about the knowledge and expertise of leaders of ISIS regarding the command-and-control environment. As the organization's command and control body, the ISIS leadership cadres had considerable knowledge and experience due to most of the leading cadres of which were former Baathist officers of Saddam Hussein's army and police. They had gained sufficient combat experience and training from various battlefields such as Iran-Iraq War, Iraq-Kuwait War, and Gulf War since the 1980s. Moreover, they had spent time in US detention centers like Camp Bucca, Camp Cropper, and Abu Ghraib prison, where they turned into a terror academy for these leaders. Again, some of the cadres were al-Qaeda-linked militants who fought against the American invasion, and some Chechens who were qualified warriors that had been fighting against the Russian army for years could become leaders of the organization with their extensive knowledge about guerilla warfare.

The second and third prerequisites (operational picture and information flow) outlined an image consisting of the activities of *Amniyat* and the security units of the organization. These units were in charge of collecting and analyzing intelligence, deploying spies, carrying out counterintelligence operations, and they contained surveillance departments, technology specialists, and economic intelligence bodies. The organization could reach detailed information and gather intelligence from Iraq and Syria via *Amniyat* and its four separate branches having specific duties in the security circle. In addition to these security units, the group had opened a *Da'wah* office, which conducted missionary activities, employed informants, and gathered information from villages, providing to the group information flow and intelligence from local tribes and other armed actors.

The fourth prerequisite (confidence/trust) focused on the trust among the leading cadres and the methods used in the command-and-control environment. The organization's inner circle consisted of one hundred percent of Iraqis who paid allegiance to the caliph and won the caliph's confidence thanks to their qualities and ability to manage tasks. Baghdadi selected the ones who had adequate knowledge about rules of engagement, experience in command-and-control environment, and Iraqi nationality for his inner circle. However, the involvement of jihadi militants had posed a danger to ISIS because a dispute or social disagreement that might arise

between these militants and former Baath officers would cause a lack of confidence and disorder that would spread to the whole organization. The methods applied and the technologies used in the command-and-control environment by ISIS were mostly communications instruments. Via these instruments, the group directed and controlled its followers, supporters, and fighters from all over the world.

The fifth prerequisite (situation awareness) clarified whether the leaders of the organization had a correct understanding of the situation within the scope of the capacity of information they had. The leaders of ISIS were former Baathist officers of Saddam Hussein's army, intelligence, and police officers with deep knowledge and experience regarding the command-and-control environment. Namely, they had situational awareness and had concrete objectives (the sixth prerequisite) respecting the establishment of a caliphate and uniting the whole Muslims under the Sharia Law, and they established a highly systematic hierarchical structure to achieve these objectives. As for the seventh prerequisite (feedback), it was ambiguous that the cadres of the Islamic State received adequate feedback from the command-and-control system. The group concentrated on carving an almighty image to intimidate and deter its enemies. It had fighters/lone wolves acting independently from all over the world, and whatever the scale of their attacks, the organization which gave importance to the spread of fear and terror was pleased with these attacks.

The ISIS cadres had the flexibility (the eighth prerequisite) could adapt to the situation they were in. The transition between the borders of Syria and Iraq and the capability to conduct operations in both countries simultaneously demonstrated the group's flexibility in adjusting itself in changing situations and varying territories. Each administrative organ of ISIS had the authority in the decision-making process (the ninth prerequisite) within the area of its duties and responsibilities; however, the ultimate decision-maker was the caliph. Even though the *Shura* council was a supreme body where critical issues and decisions were discussed, the ultimate decision-maker was Baghdadi, who had an absolute and unlimited command and control authority over the entire organization.

The meeting of most of the nine prerequisites of command-and-control ability for ISIS was an indication that the jihadi group could operate its command-and-control

warfare effectively. Moreover, the capturing strategic provinces like Mosul and Raqqa showed that the organization had a considerable command and control ability that could compete with states like Iraq and Syria.

### 4.1.2 Psychological Warfare Capability of ISIS

ISIS sought to create a media strategy that could present an image of war that would influence public opinion and penetrate the hearts and minds of people. The group took advantage of both traditional and media tools in line with several objectives. Those were establishing legitimate political and religious authority, threatening its adversaries, penetrating the minds and hearts by inserting its ideas, recruiting new fighters, communicating with its supporters from all around the world, and presenting an omnipotent image that would create fear and unrest among people.

The group's media strategy had split into two branches: traditional media and social media. Having its official media organs such as Al-Hayat Media, *Dabiq* and *Rumiyah* Magazines, *Al-Furqan* Foundation, *Ajnad* Foundation, *Al-Himmah* publications, *Al-Naba* newsletter, Al-Bayan Radio, and *Wilayat* Media offices was an indication that the group had a comprehensive media strategy and policy. The Islamic State utilized conventional media tools like audio statements, magazines, videos, news reports, and *nasheeds* with contents of violence, fighting, religion, power, and deterrence. Featured audio statements of Baghdadi from time to time were an example that the group aimed to direct its followers and galvanize them into action by using traditional media tools. The video records regarding the executions and beheadings of international citizens were the most visual platforms that astounded the whole world against ISIS's brutal actions. The group published magazines in different languages in line with its propaganda actions referring to particular contents; Islamic teaching and justification, stories of progress and heroism, the establishment of common enemies, appeal to the community, belonging and meaning, instructional and inspirational. Being two outstanding propaganda magazines of ISIS, *Dabiq* and *Rumiyah* magazines took their names from holy cities giving a direct message to its adversaries and the international community. The group recruited a professional class staff to conduct and

sustain its propaganda actions through media apparatuses, including hundreds of videographers, producers, and editors responsible for scripting, filming, cutting, and disseminating ISIS films. That illustrated how professionally the group managed its media strategy.

On the other hand, the group was skillful as far as it could on social media platforms. ISIS members and supporters used social media platforms such as Twitter, Facebook, and YouTube in line with their media objectives, and they were successful to a great extent. On Twitter, the group put to use at least 46.000 Twitter accounts over a four-month period from December 2014 to March 2015. Twenty percent of Twitter accounts of ISIS supporters handled these accounts in the English language, while seventy-five percent of these accounts run in the Arabic language. Additionally, each account supporting ISIS had nearly one thousand followers that an average Twitter user had less than these followers. Besides, the group disseminated their traditional media products such as audio statements, brutal videos via YouTube, Facebook, and Twitter platforms. By using such social media platforms, the group had the opportunity to propagate its heinous and deviant thoughts more quickly. ISIS was quite so well-skilled at using internet platforms, especially social media, and conducting its propaganda actions through these platforms that efforts to prevent ISIS from using these platforms as its propaganda machine had been relatively futile (Lieberman, 2017, p. 95).

The effective and prosperous usage of both traditional media tools and modern media apparatuses, mainly social media platforms, by ISIS followers\supporters and militants, had created fear and anxiety at the international level. The efforts, including deletion of their online content, suspension of social media accounts, and hacking the group's websites, performed by the United States aimed at preventing the usage of social media and other media platforms by ISIS followers\supporters\militants, failed. Because the group swiftly adopted this situation and carried their propaganda networks to other encrypted communication channels and platforms such as Telegram, Signal, WhatsApp, and Justpaste.it, Sendvid.com, and Dump.to. By this means, the group continued its activities on other internet platforms, and the attempts to destroy and hinder the group's activities fell through.

Targeting all Muslims, the group's supporters/followers, and western media, and its enemies, media products of the Islamic State both became narratives that inspired its supporters and portrayed a threat against the international community that accepted ISIS as a tough terrorist organization and tried to struggle with the organization. On the other hand, the group had noticed the power of social media platforms such as Twitter, Facebook, and YouTube and began to benefit from them effectively, and it had established and managed a highly successful social media network. Such that, the organization gathered scores of new militants from all over the world, albeit a considerable number of them had come from Western countries.

### 4.1.3 Cyberwarfare Capability of ISIS

ISIS benefitted from cyberspace as part of unconventional warfare because cyberspace was so convenient for the organization in terms of cost and expenses. Carrying the aim of spreading its ideology, generating fear and anxiety, perplexing human minds, conducting all sorts of propaganda, manipulation, and disinformation campaigns upon populations and governments, the Islamic State pursued mainly four strategies while exploiting from cyber domain; recruitment strategy, intimidation strategy, provocation strategy, and outbidding strategy.

In recruitment strategy, ISIS hackers sought to find potential recruits by hacking users' social media accounts to find out jihadi-inclined individuals and access their personal information such as name, place of birth, phone numbers, addresses, and employee records. ISIS hackers communicated with these potential recruits and relayed the group's messages via sophisticated computer games. Besides, the group tried to attract supporters\followers with video games involving savage images that showcased their atrocious and extreme thoughts.

In intimidation strategy, the group aimed to create unrest among the international community by spreading fear through cyber-attacks in which they hacked several websites of businesses, religious groups, universities, municipalities and shared their ill-intentioned messages that stunned the world.

In provocation strategy, ISIS hackers executed cyber-attacks on some strategic government infrastructures belonging to several countries from the United States, the United Kingdom, and French to Australia to challenge these countries and show their ability to the world what it would do. Among the infrastructures attacked by ISIS, American electrical power companies, the social media accounts of CENTCOM, Government Communications Headquarters of the United Kingdom, an Australian airport were salient instances illustrating the organization wielded cyberspace as part of its information warfare campaign. In spite of these cyber-attacks against notable infrastructures, they had just short-term effects and failed to cause permanent and irreparable damage. Nevertheless, the attacks aroused concerns for future cyber-attacks. The probability that the group would successfully perform various cyber-attacks in the future found a place among specialized institutions and individuals in the field. A software company had claimed that ISIS would be able to carry out significant cyber-attacks against critical infrastructures and bureaucrats in the future if it augmented its cyber capability. On the other hand, the FBI had proclaimed that in case ISIS possessed malicious software that could sneak into computers and destroy power companies would result in a damaging flow of energy to homes and businesses.

In its outbidding strategy, the group activated its passive followers to active members to perform terrorist actions in parallel with its recruitment strategy towards recruiting new members for the organization. Also, as a result of the outbidding strategy of ISIS, these new attendants had turned into lone wolves and organized independent attacks like the 2015 Paris and the 2016 Brussels attacks.

### 4.1.4 Economic Warfare Capability of ISIS

Conducting most of its economic activities in its dominated lands, the Islamic State also gained most of the revenues from these lands. Pretending like a state, the group collected taxes, fees, and extortions from the local people. The local inhabitants obeyed and consented to ISIS's rule because of the unstable and conflict environment that Iraq and Syria were in and the failure of the governments of these countries to provide these inhabitants with necessary economic conditions. The Islamic State,

albeit at a low level, ensured requirements and aid programs to these local people to earn their livelihood compared with the governments of Iraq and Syria.

ISIS had colossal wealth at its heyday. According to a list created by Forbes Israel, ISIS was the richest terrorist organization the world has known (Forbes International, 2014). The significant incomes of ISIS consisted of revenues obtained from taxes and fees, looting and confiscations, oil and gas sales, kidnapping for ransom, sale of antiquities, foreign donations, extortions, robbery, looting, and fines. Besides, the revenues from the operation of agricultural lands, dams, strategic facilities, and mineral deposit reserves in occupied territories were other revenue items of the terrorist organization. Again, the group used revenues it earned to cover its expenses and finance its goals, such as expanding to other regions.

Because ISIS obtained its funds in its own territory, the efforts, such as international cooperation regarding exchanging information and freezing the group's assets, aimed at terminating the fund flow of the organization, were not functional. Therefore, the most disruptive way to demolish its financial circulation was to attack its economic facilities and get ISIS out of the region. Likewise, the revenues of the group decreased as a result of the air campaign organized by the US aimed at bombing the oil and gas assets and supply chain of the group. On the other hand, to compensate for its loss of income, the Islamic State resorted to imposing additional charges on the local population and taking measures such as reduced salaries of fighters, boosted tax receipts and fines, reduced aid programs, and extended electricity cuts on the local population.

Due to ISIS was not a legal entity but a terrorist organization, it had no voice in any legitimate economic system involving many legitimate actors. Therefore, it had not an essential capability to the deliberate use of economic assets against overt hostilities in line with its interests. Then again, because the Islamic State was not integrated into the multiple economic and financial systems, it was out of the question for the terrorist group to be exposed to economic attacks, take countermeasures against them, or make economic attacks through economic assets. For example, ISIS could not afford to use the main tools of economic warfare such as embargoes, boycotts, blockades, sanctions, or economic strikes to suppress its adversaries, as its adversaries

could not. Nevertheless, it imposed tariffs on imports to a great extent, and it took under the control oil fields. Under its rule, the group operated these fields like a state oil company, employed skilled workers and engineers in its oil installation, and deployed militants to shield its oil fields and staff. Again, by using tariffs and holding control of oil exports as tools of economic warfare, the Islamic State was not competent to able to dominate strategic economic industries.

### 4.1.5 Electronic Warfare Capability of ISIS

The Islamic State had achieved significant success in a short time by seizing a remarkable territory of Iraq and enlarging its lands to Syria, where it would later declare Raqqa as the capital of its caliphate. Moreover, especially in Iraq, it captured a large amount of weaponry and ammunition that the Iraqi army had left behind while withdrawing and escaping from ISIS. The appearance of a Scud missile, which is a long-range ballistic missile and complex systems carrying weapons systems with radar and a nuclear head, was evidence that ISIS had seized an electronic weapon that predicted it would capture from the Iraqi army. However, the organization's electronic capacity mostly rested on low-tech apparatus such as communication tools and drones. Additionally, a laptop belonging to a member of the Islamic State, which included several pages of documents regarding biological weapons, brought into open that the organization had paid attention to WMD. The acquisition of remnants of rockets filled with sarin and other deadly nerve agents from the Muthanna complex and nuclear materials, including uranium compounds from Mosul University, had indicated the organization took care of nuclear weapons. In other respects, the communication systems and cyberspace by which the group also conducted psychological and cyber warfare were other tools of electronic warfare for ISIS. Again, there were some claims that the group tried to develop some electronic and nuclear weapons but, it was uncertain whether the Islamic State had sufficient technical personnel and know-how.

Having such tools as drones, missiles, reconnaissance and surveillance tools, communication satellites and systems, space weapons, nuclear weapon systems, and command and control systems has been necessary to run electronic warfare. However,

ISIS's possession of the before-mentioned electronic tools was at such a pretty low level that although it actualized assaults via its low-tech electronic devices, it hardly ever provided electronic protection for itself against the assaults practiced by any electronic devices.

The Islamic State exploited drones predominantly for the purpose of immediate threat recognition, collecting imagery intelligence, filming its operations, detections, analysis, reconnaissance, and surveillance to provide itself electronic support. It benefitted from drones to get under control of the electromagnetic environment against the actions of the hostile powers. Furthermore, the drones equipped with small munitions with an approximate explosive power of small hand grenades for the group were devices that were used to carry out assaults against target personnel and facilities to degrade and neutralize them.

Due to the deficiency sources and knowledge regarding the electronic warfare capacity of ISIS, it was not clear precisely whether the group had advanced electronic tools that would compete with or cope with the states. The group had capitalized on low-tech electronic devices in terms of electronic warfare. Although there were few nonsignificant allegations that the group had missile and CNBRN weapons, there were limited examples to support allegations. Even if the allegations were correct, ISIS was unlikely to have the capacity to compete with states given the possibilities and capabilities to possess electronic means.

### 4.2 The Evaluation of The Information Warfare Capability of ISIS

In order to demonstrate the information warfare capability of ISIS as an NSAA, the research attempted to answer the five sub-questions (determined in the introduction chapter of the study) in the third chapter in line with the theoretical framework in the second chapter. The research sub-questions were 1- Can the command-and-control ability of an NSAA compete with states? 2- Does an NSAA successfully use traditional and modern methods while conducting psychological operations? 3- Has an NSAA become a threat to states in terms of cyber warfare? 4- Could an NSAA engage in economic warfare with the states? 5- Does an NSAA have sufficient electronic warfare

capacity in terms of the electromagnetic spectrum to a certain extent? In this regard, the thesis tried to reply to these sub-questions in light of the above findings.

1. Can the command-and-control ability of an NSAA compete with states?: In order to measure the command-and-control ability of ISIS, the study focused on nine prerequisites of command-and-control warfare: knowledge and experience, operational picture, trust, information flow, situational awareness, objectives, feedback, flexibility, and decision making. According to research findings,

— Most of the ISIS leadership cadres consisted of former Baathist officers of Saddam Hussein's army and police who had gained sufficient combat experience and training from various battlefields since the 1980s and spent time in US detention centers _which turned into terror academies for them_ after the invasion of Iraq. So, they had relevant knowledge and experience regarding the command-and-control environment. ISIS had *Amniyat*, the security units, and the *Da'wah* office, which were in charge of collecting and analyzing intelligence, deploying spies, carrying out counterintelligence operations, and contained surveillance departments and technology specialists, and economic intelligence bodies. These bodies illustrated that the terrorist organization met its own operational picture and information flow needs. Although the inner circle of ISIS consisted of one hundred percent of Iraqis because of the distrustfulness of Baghdadi, the involvement of jihadi militants in other structures of the organization posed a danger to ISIS because of a disagreement or social disagreement that would occur among the organization's cadres. The technology used in the command-and-control environment by ISIS was mostly communications instruments that provided communication between members. Namely, the Islamic State could not exactly meet confidence\trust prerequisite. Because the leaders of ISIS were former Baathist officers of Saddam Hussein's army, intelligence, and police officers with deep knowledge and experience regarding the command-and-control environment, they had the correct understanding of their situation. Also, the establishment of a caliphate and uniting the whole Muslims under the Sharia Law was the main and explicit purpose of ISIS. So, it means that ISIS carried situation awareness and objectives prerequisites. The issue that ISIS actors received adequate feedback from the command-and-control environment was ambiguous. Because although the group had a hierarchical structure, it also had independent cells and

followers of each other that acted on behalf of the group without ISIS attachment. ISIS fighters shuttled back and forth between Iraq and Syria and carried out simultaneous operations in both countries, and the group achieved to seize the cities of Iraq in, such as Fallujah, Ramadi, and Mosul a short period and declared the Syrian city of Raqqa as the capital of the caliphate. Within the area of its duties and responsibilities, although each administrative organ of ISIS had the authority in the decision-making process, the ultimate decision-maker was the caliph. So, it was unclear whether decisions were taken effectively, appropriately, and made with adequate swiftness.

To be more precise, ISIS provided the prerequisites of knowledge and experience, operational picture, information flow, situation awareness, objectives, and flexibility. However, it was unclear whether ISIS provided the other prerequisites of command-and-control. The most crucial point proving an answer to the sub-questions was that the group achieved to seize the cities of Iraq in, such as Fallujah, Ramadi, and Mosul a short period and declared the Syrian city of Raqqa as the capital of the caliphate. That means, because ISIS provided the most prerequisites of command-and-control ability, it had the command-and-control ability to compete with states like Iraq and Syria.

2. Does an NSAA successfully use traditional and modern methods while conducting psychological operations?: Given that ISIS had followed a media strategy consisting of both traditional and modern methods, the sub-question strived to indicate whether ISIS successfully used traditional and modern methods while conducting psychological operations depending on the following findings.

— ISIS sought to allocate an image of war based on a media strategy consisting of both traditional and modern methods. The group had its official media bodies. Through them, it utilized various traditional media products such as audio statements, videos, magazines, *nasheeds*, and news reports with violence, fighting, religion, power, and deterrence contents. Audio statements were the transmitters by which ISIS relayed its messages to supporters\followers, militants and enemies. The video records were the most visual platforms that astounded the whole world against ISIS's brutal actions. *Dabiq* and *Rumiyah* were two outstanding magazines of ISIS published in several different languages and focused on the subject of Islamic teaching and

justification, heroism, the establishment of common enemies, belonging, and meaning, instructional and inspirational. The organization also benefitted from *nasheeds* involving religious messages and narratives and news reports composed of pictures or infographics involving visual messages that contributed to the group's image war. The fact that ISIS employed highly professional staff, including videographers, producers, and editors responsible for scripting, filming, cutting, and disseminating ISIS films, was evidence of how professionally ISIS handled the traditional media tools.

— In the same manner, ISIS was rather talented in using modern tools of psychological warfare, especially social media. ISIS had effectively utilized social media platforms like Twitter, Facebook, and YouTube. A report released by Brookings Institution in 2015 regarding defining and describing the population of ISIS supporters on Twitter illustrated how the ISIS followers used at least 46.000 Twitter accounts with different languages, including Arabic and English, over a four-month period astounded the whole world. Besides, the group propagated the contents and products of its traditional media bodies on these social media platforms. In this way, the group had aimed to increase the audience and gain more followers and supporters. Effective use of these media apparatus astounded the international community and forced them to take action against ISIS's activities, especially on social platforms. The efforts, including deletion of their online content, suspension of social media accounts, and hacking the group's websites, performed by the United States were futile. The group quickly adapted to the new situation and carried their propaganda networks to other encrypted communication channels and platforms such as Telegram, Signal, WhatsApp, and Justpaste.it, Sendvid.com, and Dump.to. Thus, the group continued its propaganda actions and gathered scores of militants worldwide via these platforms. So those means that ISIS successfully used traditional and modern methods while conducting psychological operations.

3. Has an NSAA become a threat to states in terms of cyber warfare?: Being aware of the power of cyberspace, ISIS tried to take advantage of cyberspace which is a new domain of warfare after land, air, and sea. Therefore, the study sought to understand whether ISIS became a threat to states in terms of cyber warfare.

— The Islamic State followed mainly five strategies in its cyber warfare: Recruitment strategy, intimidation strategy, provocation strategy, and outbidding strategy. ISIS hackers benefitted from cyberspace to access the name, places of birth, phone numbers, addresses, and employee records of potential recruits and induce them to participate in the group. In tandem with the recruitment strategy, the outbidding strategy of the group relied on recruitments to turn passive supporters into active fighters such as lone wolves to organize independent and resounding attacks around the world. However, psychological operations rather than operations in cyberspace had been effective in recruitments of ISIS. In its intimidation strategy of the group, ISIS hackers attempted to disseminate fear and anxiety by sharing their deviant and threatening messages through cyberspace. As for its provocation strategy, even though ISIS hackers attacked some strategic government infrastructures belonging to several countries from the United States, the United Kingdom, French to Australia and targeted individuals\bureaucrats, these cyber-attacks had short-term effects that did not cause irreparable damages. That means that ISIS did not become a threat to states in terms of cyber-warfare. However, there were some allegations that in case ISIS possessed malicious software and augmented its cyber capability, it would have carried out significant cyber-attacks against critical infrastructures and been a threat to states.

4. Could an NSAA engage in economic warfare with the states?: In order to find out the response to the question, the study presented a general framework about the economy of ISIS and reached a conclusion according to the following findings.

— The economy of ISIS was predicated on the lands it occupied and dominated to a large scale. The group acted as a state and collected taxes, fees, and extortions from the local population. Again, ISIS carried out economic activities such as oil and gas sales, kidnapping for ransom, sale of antiquities, looting, and confiscations in these lands. However, it could not be included in the legitimate economic system because of its illegal nature. Therefore, it had not an essential capability to the deliberate use of economic tools such as embargoes, boycotts, blockades, sanctions, or economic strikes. Although it imposed custom duties on imports from the territories under its control, this was not sufficient to be an indication that it would conduct economic warfare. In a word, ISIS as an NSAA could not engage in economic warfare with the states.

5. Does an NSAA have sufficient electronic warfare capacity in terms of the electromagnetic spectrum to a certain extent?: In order to answer the question, the above findings regarding the electronic warfare capability of ISIS were obtained from the information given in the third section. According to these findings;

— In terms of electronic capacity, ISIS had a Scud missile on a large scale. The other electronic devices used by the group consisted of low-tech devices such as communication tools and drones. Although the group paid attention to developing WMD, there was no concrete evidence that it had succeeded. It is essential to acquire such tools as drones, missiles, reconnaissance and surveillance tools, communication satellites and systems, space weapons, nuclear weapon systems, command and control systems for having a remarkable electronic warfare capacity. However, considering the low-tech devices above-mentioned ISIS had, it did not have sufficient electronic warfare capacity in terms of the electromagnetic spectrum.

# 5. CONCLUSION

The information warfare concept involves a process of defending information, attacking information, and exploiting information in a variety of ways. It is also a strategic warfare to provide a competitive advantage over other elements to defend, attack, and protect by benefiting from information systems and technologies. Although it has been applied as a war strategy since ancient times, it gained importance as of the twentieth century and has become a battlefield at the strategic, operational, and tactic level for both states and non-state actors. In this sense, the study aimed to examine the information warfare capability of an NSAA over a case based on the concept of information warfare. By doing so, the study purposed of presenting a new perspective for the information warfare concept by measuring the information warfare capability of an NSAA. At the same time, it aimed to contribute to the academic literature by measuring the ability of NSAA on this issue.

ISIS was chosen as a case for study because, by nature, that combined both conventional war and unconventional war methods and founded a ground for itself in an asymmetrical and hybrid warfare environment. The study mainly handled five types of information warfare and inserted them into the information warfare of ISIS to deal with research questions. After information given in the second chapter regarding the concept and types of information warfare, _command and control, psychological, cyber, economic, and electronic warfare_ the study investigated the information warfare of ISIS in the third chapter. Then, based on inferences from information given in this chapter, the study obtained research findings and tried to answer research sub-questions in light of these findings in the fourth chapter.

The first sub-question was Can the command-and-control ability of an NSAA compete with states? Taking control of cities like Fallujah, Ramadi, and Mosul in a short time and declaring Raqqa as the capital of the caliphate, and being able to carry out simultaneous operations in both countries demonstrated that the group had a substantial information warfare capability that would compete with the states such as Iraq and Syria in terms of its command-and-control warfare. As a matter of fact, the conflict and chaos that Iraq and Syria were in had prepared the ground for ISIS to take

over these cities smoothly. Nonetheless, it can be said that in states where there is instability, turmoil, and chaos, an NSAA like ISIS can have the command-and-control ability to compete with states.

The second sub-question was Does an NSAA successfully use traditional and modern methods while conducting psychological operations? ISIS had achieved in penetrating the minds and hearts of people, enticing them to recruit and threatening the international community through complex and versatile media strategy that wielded effectively both traditional and social media tools, especially internet platforms as a part of its psychological warfare. The group was so skilled at using internet platforms that it continued to benefit from them as a propaganda machine despite the efforts to prevent the group from using them. Ultimately, it has been revealed that an NSAA can successfully use traditional and modern methods while conducting psychological operations.

The third sub-question was, Has an NSAA become a threat to states in terms of cyber warfare? ISIS's capacity to exploit cyberspace was immature. It followed productive actions by using cyberspace in recruiting new members and turning passive supporters into active ones; however, it failed to perform large-scale cyber-attacks because of its relatively limited cyber capacity. However, there were predictions that it would pose a threat to states, in case it would have malicious software and improve its cyber capacity. In the light of these findings, an NSAA does not become a threat to states in terms of cyber warfare as it stands; nonetheless, this does not mean that it will not pose a threat to states in the future.

The fourth sub-question was Could an NSAA engage in economic warfare with the states? As the main objective of economic warfare, neutralization of the enemy's economic and financial systems by using economic tools such as tariffs, blockades, sanctions, and embargoes, was not a convenient method for ISIS to conduct economic warfare due to its illegal nature that deprived it of inclusion in any legitimate economic and financial system. Accordingly, an NSAA cannot have the ability to engage in economic warfare with states.

Lastly, the fifth sub-question was Does an NSAA have sufficient electronic warfare capacity in terms of the electromagnetic spectrum to a certain extent? Due to

a lack of acquired sources, knowledge, know-how, and technicians, the Islamic State had no capability to develop advanced electronic devices and weapons based on the electromagnetic spectrum to pursue electronic warfare. Although it exploited some low-tech devices like drones and communication tools, it was not adequate to conduct electronic warfare. That means an NSAA does not have sufficient electronic warfare capacity in terms of the electromagnetic spectrum.

The main research question of the study was, does an NSAA have information warfare capability? As can be understood from the information given in the third chapter and the findings obtained in the fourth chapter, the talent of ISIS in conducting command and control warfare and psychological warfare and the using cyberspace and electromagnetic environment as a theater of war, albeit at a low-level, have revealed that ISIS had the information warfare capability to a certain extent.

The following research question was, does an NSAA have any superiority over states in terms of information warfare capability? The hallmark of ISIS in information warfare was due to its success in command-and-control and psychological warfare capability. ISIS had an immature cyber and insufficient electronic capacity that prevented it from conducting considerable information warfare in terms of cyber and electronic warfare. Additionally, it was also not integrated into the legitimate economic systems necessary to wage economic warfare. Considered as a whole, ISIS did not have superiority over states in terms of information warfare capability. The fact that the success of ISIS in waging command and control warfare and psychological warfare did not mean that it would compete with states regarding information warfare. All in all, ISIS had no remarkable capability in the other three types of information warfare. Hence, ISIS could not compete with states regarding information warfare.

In this regard, the following results emerged from the research questions based on the ISIS case; an NSAA can have information warfare capability. However, an NSAA does not have superiority over states in terms of information warfare capability, and it cannot compete with states regarding information warfare.

It is an incontestable fact that ISIS has left its mark in history by combining unconventional methods of war in addition to conventional ones as an NSAA. Even

though the group began to lose its influence as of late 2016 as a result of the global coalition's assaults that started in 2014, the resurgence of the group is possible in the future, as seen in the example of the Taliban. Taliban had emerged after the Soviet Invasion of Afghanistan in 1979 and took control of Afghanistan from 1996 to the US invasion of Afghanistan in 2001. As a result of the invasion, the Taliban administration was toppled down but, it has somehow continued its existence. Almost twenty years have passed since then, Taliban has gotten back to the stage; it has regained control of Afghanistan as of August 2021 by compromising with the United States. Likewise, ISIS is not entirely dead out; it still comes on the stage from time to time with attacks it carries out in different states such as Iraq, Afghanistan. Taking into account its past knowledge, ability, and experience of ISIS, there is a possibility that the group will reorganize by developing its information warfare capability and become more powerful than before, as in the case of the Taliban. Namely, if ISIS can manage to resurgence and have more information-based capability, it will likely be a threat to the international community.

Information warfare is a general concept that includes an extensive area. This study discussed the subject in terms of the information warfare capability of an NSAA by handling the primary five types of information warfare and placing them into those of ISIS as a case. The feature that distinguishes this study from other studies on information warfare is that other studies concentrated on one type of information warfare, for the most part of psychological warfare or cyber warfare of NSAAs, while this study handled the subject around more than one type of information warfare and tried to evaluate NSAAs from another point of view except for conventional aspect.

Decisive studies pertaining to the economic and electronic warfare of ISIS have not been directly involved in literature, and so the resources relevant to the economic and electronic warfare of ISIS as an NSAA were limited. Also, because ISIS is not a legitimate entity is a cause that the resources regarding economic and electronic warfare are fewer. Therefore, this study could not adequately address the economic and electronic warfare of ISIS. On the other hand, although this study addressed the main five types of information warfare, there are other types of information warfare, such as hacker and intelligence warfare, as Libicki examined. This study dealt with hacker warfare under cyber warfare and intelligence warfare under command and

control warfare over ISIS without going deep into the subject. Making prospective studies regarding these issues will complete the deficiencies of the study and enable better analysis regarding the capabilities of NSAAs in terms of information warfare.

Furthermore, the recapture of Afghanistan by the Taliban can be evaluated within the context of its information warfare capability of an NSAA as another case. Especially it can be investigated within the frame of intelligence warfare which is another type of information warfare. This will bring a new perspective to the issue of how the Taliban regained control of Afghanistan. The examination of whether the Taliban conducted any information warfare consisting of its past knowledge and experience of the recapture of Afghanistan, will be significant in terms of illustrating whether the information warfare affected its success.

## REFERENCES


Ackerman, S. (2015, January 12). *US Central Command Twitter account hacked to read 'I love you Isis'*. Retrieved June 7, 2021, from the Guardian: http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack

Ackerman, S., MacAskillin, E., & Ross, A. (2018, August 27). *Junaid Hussain: British hacker for Isis believed killed in US air strike*. Retrieved June 7, 2021, from the Guardian: http://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike

Ağar, A. (2015). *Işid ve Irak: Beled el-nifak vel şikak!: İkiyüzlülüğün ve düşmanca ayrılığın diyarı! - Hz. Ali* (1st ed. ed.). Etiler, İstanbul: Remzi Kitabevi.

Akbar, J. (2015, January 15). *'Death to France. Death to Charlie': Pro-ISIS hackers launched 'unprecedented' wave of cyber-attacks on 19,000 French websites*. Retrieved June 7, 2021, from Mail Online: https://www.dailymail.co.uk/news/article-2912280/Death-France-Death-Charlie-Pro-ISIS-hackers-launched-unprecedented-wave-cyber-attacks-19-000-French-websites.html

Al Jazeera. (2014, July 2). *Iraq's Baghdadi calls for 'holy war'*. Retrieved June 7, 2021, from Al Jazeera: https://www.aljazeera.com/news/2014/7/2/iraqs-baghdadi-calls-for-holy-war

Al Jazeera Türk. (2016, September 7). *5 soruda Rakka- Ortadoğu, Kafkasya, Balkanlar, Türkiye ve çevresindeki bölgeden son dakika haberleri ve analizler*. Retrieved June 7, 2021, from Al Jazeera Türk: http://www.aljazeera.com.tr/al-jazeera-ozel/5-soruda-rakka

Alkaff, S. (2014). Abu Bakr Al-Baghdadi, the Imposter. *Counter Terrorist Trends and Analyses, 6*(10), 4-7. Retrieved from https://www.jstor.org/stable/26351289

Allen, R. (1959). State Trading and Economic Warfare. *Law and Contemporary Problems, 24*(2), 256-275. doi:10.2307/1190336

Aymenn Jawad Al-Tamimi's Blog. (2015, May 2). *"We have the Swords"- Nasheed from Islamic State's Ajnad Media.* Retrieved June 7, 2021, from Aymenn Jawad Al-Tamimi's Blog: https://www.aymennjawad.org/2015/05/we-have-the-swords-nasheed-from-islamic-state

BBC News. (2014, July 9). *Iraq confirms rebels seized Muthanna chemical arms site: BBC News*. Retrieved from BBC News: https://www.bbc.com/news/world-middle-east-28222879

BBC News, Foley beheading video shocks the world, Obama says, BBC News. (2014, August 20). *Foley beheading video shocks the world, Obama says*. Retrieved June 7, 2021, from BBC News: https://www.bbc.com/news/world-middle-east-28867627

BBC News, Trump: 'Abu Bakr al-Baghdadi is dead'. (2019, October 27). *Trump: 'Abu Bakr al-Baghdadi is dead'.* Retrieved June 4, 2021, from BBC News: https://www.bbc.com/news/av/world-50200383

Benmelech, E., & Klor, E. (2020). What Explains the Flow of Foreign Fighters to ISIS? *Terrorism and Political Violence, 32*(7), 1458-1481. doi:10.1080/09546553.2018.1482214

Berger, J., & Morgan, J. (2015). *The ISIS Twitter census: defining and describing the population of ISIS supporters on Twitter.* Washington D.C: Brookings Institution; The Brookings Project on U.S. Relations with the Islamic World. Retrieved from https://apo.org.au/node/53568

Bērziņš, J. (2014). Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy. *National Defence Academy of Latvia Center for Security and Strategic Research*, 2002-2014. Retrieved from https://www.sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

Besenyő, J. (2016). The Islamic State and its human trafficking practice. *Strategic Impact:*(3), 15-21.

Blannin, P. (2017, 9 5). Islamic State's Financing: Sources, Methods and Utilisation. *Counter Terrorist Trends and Analyses, 9*(5), 13-22.

Burnett, S. (2014, July 10). *Iraqi 'Terrorist Groups' Have Seized Nuclear Materials: Time*. Retrieved June 7, 2021, from Time: https://time.com/2972050/iraq-terrorist-nuclear-materials-isis/

Carter, C. (2014, August 20). *ISIS beheading U.S. journalist James Foley, posts video*. Retrieved June 7, 2021, from CNN: https://www.cnn.com/2014/08/19/world/meast/isis-james-foley/index.html

Chulov, M. (2014, December 11). *Isis: the inside story*. Retrieved June 7, 2021, from The Guardian: https://www.theguardian.com/world/2014/dec/11/-sp-isis-the-inside-story

Clarke, K., & Kocak, K. (2020). Launching Revolution: Social Media and the Egyptian Uprising's First Movers. *British Journal of Political Science*, 1025-1045. doi:10.1017/S0007123418000194

Cockburn, P. (2014). *İslam Devleti'nin yükselişi: İşid ve yeni Sünni ayaklanması* (1st ed. ed.). (O. Akınhay, Trans.) Agora Kitaplığı.

Cornish, P., & Yorke, D. (2010). *On Cyber Warfare.* London: The Royal Institute of International Affairs (Chatham House). Retrieved June 4, 2021, from https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf

Counter Extremism Project. (n.d). *Omar al-Shishani*. Retrieved June 7, 2021, from Counter Extremism Project: https://www.counterextremism.com/extremists/omar-al-shishani

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed ed.). Thousand Oaks, CA: SAGE Publications.

Cumhuriyet. (2014, July 3). *'IŞİD o füzelerle Ankara'yı vurur': Cumhuriyet*. Retrieved June 7, 2021, from Cumhuriyet: https://www.cumhuriyet.com.tr/haber/isid-o-fuzelerle-ankarayi-vurur-89881

Curry, C. (2014, June 10). *Iraq's Army Left Weapons Like These in the Hands of Terrorists Today*. Retrieved June 7, 2021, from ABC News: https://abcnews.go.com/International/iraqi-army-left-weapons-hands-terrorists-today/story?id=24070848

Dictionary.com. (2020, May 15). *"Misinformation" vs. "Disinformation": Get Informed On The Difference*. Retrieved June 8, 2021, from Dictionary.com: https://www.dictionary.com/e/misinformation-vs-disinformation-get-informed-on-the-difference/

Doornbos , H., & Moussa, J. (2014, August 28). *Found: The Islamic State's Terror Laptop of Doom: Foreign Policy*. Retrieved June 7, 2021, from Foreign Policy: https://foreignpolicy.com/2014/08/28/found-the-islamic-states-terror-laptop-of-doom/

Ellis, R. (2015, May 14). *ISIS releases audio of leader al-Baghdadi*. Retrieved June 7, 2021, from CNN: https://www.cnn.com/2015/05/14/asia/al-baghdadi-audio/index.html

European Parliament, Directorate-Gen.l for External Polic. of the Union, Cousseran, J.-C., & Levallois, A. (2017). *The financing of the 'Islamic State' in Syria and Iraq (ISIS) : in-depth analysis.* Belgium: European Parliament.

Eweiss, N. (2016). Non-state actors & WMD: Does ISIS have a pathway to a nuclear weapon? *British American Security Information Council, March, 29*, 1-8.

Fadok, D. (1995). *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis.* Alabama: AIR UNIV MAXWELL AFB AL SCHOOL OF ADVANCED AIRPOWER STUDIES. Retrieved June 4, 2021, from https://apps.dtic.mil/sti/citations/ADA291621

FATF. (2015). *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant.* Paris: The Financial Action Task Force (FATF).

Fogleman, R., Widnall, S., & United States Air Force. (1997, April 17). *Cornerstones of Information Warfare.* Retrieved June 6, 2021, from National Security Archive: https://nsarchive.gwu.edu/document/15889-united-states-air-force-cornerstones

Forbes International. (2014, December 12). *The World's 10 Richest Terrorist Organizations*. Retrieved June 4, 2021, from Forbes: https://www.forbes.com/sites/forbesinternational/2014/12/12/the-worlds-10-richest-terrorist-organizations/

Freedman, L. (2014). Ukraine and the Art of Limited War. *Survival*, 7-38. doi:10.1080/00396338.2014.985432

Gerges, F. (2016). *ISIS: a history.* Princeton: Princeton University Press.

Goodman, M., & Brenner, S. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology, 10*(2), 139-223. doi:10.1093/ijlit/10.2.139

Graham-Harrison, E. (2015, April 12). *Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?* Retrieved June 7, 2021, from the Guardian: http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race

Gråtrud, H. (2016). Islamic State Nasheeds As Messaging Tools. *Studies in Conflict & Terrorism, 39*(12), 1050-1070.

Greene, K. (2015, April 24). ISIS: Trends in Terrorist Media and Propaganda. *International Studies Capstone Research Papers*, 1-58.

Haaretz, U.S. journalist beheaded by ISIS was Israeli citizen, Foreign Ministry says. (2014, September 3). *U.S. journalist beheaded by ISIS was Israeli citizen, Foreign Ministry says*. Retrieved June 7, 2021, from Haaretz.com: https://www.haaretz.com/u-s-is-video-of-journalist-beheading-is-authentic-1.5262930

Hallahan, K. (2014). Organizational goals and communication objectives in strategic communication. *The Routledge handbook of strategic communication*, 244-266.

Hallahan, K., Holtzhausen, D., van Ruler, B., Verčič, D., & Sriramesh, K. (2007). Defining Strategic Communication. *International Journal of Strategic Communication, 1*(1), 3-35. doi:10.1080/15531180701285244

Hammervik, M., Lindoff, J., Castor, M., & Tydén, L. (2007). Studying the Effects of Command and Control Warfare on Command and Control Performance. *The Swedish Defence Research Agency (FOI).* Sweden: The Swedish Defence Research Agency (FOI). Retrieved June 4, 2021

Haniyeh, H. (2014, December 3). *Daesh's Organisational Structure*. Retrieved June 7, 2021, from مركز الجزيرة للدراسات: http://studies.aljazeera.net/ar/node/1083

Hankiss, Agnes; Counterterrorism Department of the National Securi;. (2018). The Legend of the Lone Wolf. *Journal of Strategic Security, 11*(2), 54-72.

Hashim, A. (2019). The Islamic State's Way of War in Iraq and Syria: From its Origins to the Post Caliphate Era. *Perspectives on Terrorism, 13*(1), 22-31. Retrieved from https://www.jstor.org/stable/26590505

Heißner, S., Neumann, P., Holland-McCowan, J., & Basra, R. (2017). *Caliphate in decline: An estimate of Islamic State's financial fortunes.* London: International Centre for the Study of Radicalisation and Political Violence.

Hengel, M. (1989). *The Zealots: investigations into the Jewish freedom movement in the period from Herod I until 70 A.D.* Edinburgh: T. & T. Clark.

Hoffman, A., & Schweitzer, Y. (2015). Cyber jihad in the service of the Islamic State (ISIS). *Strategic Assessment, 18*(1), 71-81.

Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

Holtzhausen, D., Fullerton, J., Lewis, B., & Shipka, D. (2021). *Principles of strategic communication.* New York: Routledge.

Homeland Security Digital Library. (2007, January 25). *Joint Publication 3-13.1: Electronic Warfare.* Retrieved June 4, 2021, from Homeland Security Digital Library: https://www.hsdl.org/?abstract&did=469779

Homeland Security Digital Library, Joint Publication 3-13: Information Operations. (2014, November 20). *Joint Publication 3-13: Information Operations*. Retrieved April 6, 2021, from Homeland Security Digital Library: https://www.hsdl.org/?abstract&did=

Hughes, P. (1998, January 28). *Global Threats and Challenges: The Decades Ahead: A Statement for the Senate Select Committee on Intelligence.* Retrieved June 4, 2021, from Homeland Security Digital Library: https://apps.dtic.mil/sti/citations/ADA350533

Hussain, M. (2016, March 23). *Islamic State Bragged That Its Attacks Would Help Break Up the European Union*. Retrieved June 7, 2021, from The Intercept: https://theintercept.com/2016/03/23/islamic-state-bragged-that-its-attacks-would-help-break-up-the-european-union/

Hutcherson, N. (1994). *Command and Control Warfare. Putting Another Tool in the War-Fighter's Data Base.* Alabama: AIR UNIV MAXWELL AFB AL AIRPOWER RESEARCH INST. Retrieved June 4, 2021, from https://apps.dtic.mil/sti/citations/ADA286005

Johnston, P. (2014). *Countering ISIL's Financing.* Santa Monica, CA: RAND Corporation.

Johnston, P., Alami, M., Clarke, C., & Shatz, H. (2019). *Return and expand? the finances and prospects of the Islamic State after the caliphate.* Santa Monica, CA: Rand Corporation.

Jowett, G., & O'Donnell, V. (2015). *Propaganda & persuasion* (Sixth edition ed.). Thousand Oaks, California: SAGE.

Kadivar, J. (2020). Exploring Takfir, Its Origins and Contemporary Use: The Case of Takfiri Approach in Daesh's Media. *Contemporary Review of the Middle East, 7*(3), 259-285: 1-27.

Khawaja, A., & Khan, A. (2016). Media Strategy of ISIS: An Analysis. *Strategic Studies, 36*(2), 104-121.

Kopp, C., Korb, K. B., & Brumley, L. N. (2012, October 20). *Cutting Through the Tangled Web: An Information-Theoretic Perspective on Information Warfare: Air Power Australia Analyses.* Retrieved June 6, 2021, from Air Power Australia Analyses: http://www.ausairpower.net/APA-2012-02.html

Larter, D. B. (2017, May 16). *SOCOM commander: Armed ISIS drones were 2016's 'most daunting problem': Defense News*. Retrieved June 7, 2021, from Defense News: https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/

Lasconjarias, G., & Maged, H. (2019). Fear The Drones: Remotely Piloted System and Non-State Actors in SYRIA and IRAQ. *IRSEM, École militaire1, place Joffre 75700 PARIS SP 07*(77), 1-20.

Lele, A. (2014). Asymmetric Warfare: A State vs Non-State Conflict. *OASIS*(20), 97-111. Retrieved from https://www.redalyc.org/articulo.oa?id=53163822007

Liang, C. (2017). Unveiling the "United Cyber Caliphate" and the Birth of the E-Terrorist. *Georgetown Journal of International Affairs, 18*(3), 11-20.

Libicki, M. (1995). *What is Information Warfare.* Washington DC.: National Defence University Press.

Lieberman, A. (2017). Terrorism, the internet, and propaganda: A deadly combination. *J. Nat'l Sec. L. & Pol'y, 9*, 95-124.

Longley, R. (2019, October 22). *An Introduction to Psychological Warfare, From Genghis Khan to ISIS.* Retrieved June 4, 2021, from ThoughtCo: https://www.thoughtco.com/psychological-warfare-definition-4151867

Macnair, L., & Frank, R. (2017). "To My Brothers in the West . . .": A Thematic Analysis of Videos Produced by the Islamic State's al-Hayat Media Center. *Journal of Contemporary Criminal Justice, 33*(3), 234-253:1-20.

Mansour, R., & Al-Hashimi, H. (2017, June 8). *ISIS and the New War Economy: Chatham House*. Retrieved June 8, 2021, from Chatham House: https://www.chathamhouse.org/2017/06/isis-and-new-war-economy

Maurer, T. (2019). ISIS's Warfare Functions: A Systematized Review of a Proto-state's Conventional Conduct of Combat Operations. *Small Wars & Insurgencies, 29*(2), 229-244. doi:10.1080/09592318.2018.1435238

McCants, W. (2015). *The ISIS apocalypse: the history, strategy, and doomsday vision of the Islamic State.* New York: St. Martin's Press.

McConnell , D., & Todd, B. (2015, August 13). *Purported ISIS militants post list of 1,400 U.S. 'targets'*. Retrieved June 7, 2021, from CNN: https://www.cnn.com/2015/08/13/world/isis-militants-american-targets/index.html

Metz, S. (2001, June 30). *Strategic Asymmetry.* Retrieved June 4, 2021, from Homeland Security Digital Library: https://www.hsdl.org/?view&did=3690

Military Review: The Professional Journal of the United States Army. (2016, January-February). *The Value of Science Is in The Foresight; New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.* Retrieved June 4, 2021, from Military Review: The Professional Journal of the United States Army: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/

Military Wiki. (n.d). *Demoralization (warfare)*. Retrieved June 6, 2021, from Military Wiki: https://military-history.fandom.com/wiki/Demoralization_(warfare)

Moore, J. (2017, September 8). *ISIS plundered $800 million from Iraq, according to the country's Central Bank: Newsweek*. Retrieved June 8, 2021, from Newsweek: https://www.newsweek.com/isis-members-plundered-800-million-iraq-central-bank-says-648492

Murray, W., & Mansoor, P. (2012). *Hybrid warfare: fighting complex opponents from the ancient world to the present.* New York: Cambridge University Press.

NBC News. (2014, July 2). *ISIS' Scud a Dud? Missile Likely Not Operational, US Officials Say: NBC News*. Retrieved June 7, 2021, from NBC News: https://www.nbcnews.com/storyline/iraq-turmoil/isis-scud-dud-missile-likely-not-operational-us-officials-say-n145916

Neagle, H. I., & Neagle, C. (2015, November 16). *How ISIS could use PlayStation 4, encrypted messaging to communicate*. Retrieved June 7, 2021, from Network World: How ISIS could use PlayStation 4, encrypted messaging to communicate

Nicolò Bussolati, An Essential Classification of Non-State Actors Operating in Cyberspace chapt, para. 1. (2015, January 1). 'The Rise of Non-State Actors in Cyberwarfare'. (J. Ohlin, K. Govern, & C. Finkelstein, Eds.) *Oxford University Press*, 102-126. Retrieved from https://papers.ssrn.com/abstract=2764185

Ockenden, W., & Sveen, B. (2016, April 15). *'Are you joking?': Small Australian businesses targeted by pro-IS hackers*. Retrieved June 7, 2021, from ABC News: https://www.abc.net.au/news/2016-04-15/pro-islamic-state-cyber-group-hack-websites-of-small-businesses/7329858

O'Leary, J. (1985). Economic warfare and strategic economics. *Comparative Strategy*, 179-206. doi:10.1080/01495938508402688

Orton, K. (2015, November 10). *The Riddle of Haji Bakr*. Retrieved June 7, 2021, from Kyle W. Orton: Medium: https://kyleworton.medium.com/the-riddle-of-haji-bakr-9a949f1c5669

Paganini, P. (2015, May 17). *ISIS – Cyber Caliphate hackers are threatening Electronic War*. Retrieved June 7, 2021, from Security Affairs: https://securityaffairs.co/wordpress/36883/cyber-crime/cyber-caliphate-electronic-war.html

Paganini, P. (2015, September 12). *ISIS hackers violated top secret British Government emails: Security Affairs*. Retrieved June 7, 2021, from Security Affairs: https://securityaffairs.co/wordpress/40077/cyber-crime/isis-violated-british-gov-emails.html

Paganini, P. (2015, October 26). *Mikko Hyppönen warns the ISIS has a credible offensive cyber capability*. Retrieved June 7, 2021, from Security Affairs: https://securityaffairs.co/wordpress/41438/intelligence/isis-offensive-cyber-capability.html

Pagliery, J. (2015, 10 15). *ISIS is attacking the U.S. energy grid (and failing)*. Retrieved June 7, 2021, from CNNMoney: https://money.cnn.com/2015/10/15/technology/isis-energy-grid/index.html

Pape, R., & Morell, S. (2015, January 25). *Four reasons for ISIS's success; OUPblog: Oxford University Press's Academic Insights for the Thinking World*. Retrieved June 8, 2021, from OUPblog: Oxford University Press's Academic Insights for the Thinking World: https://blog.oup.com/2015/01/reasons-isis-islamic-state-success/

Pellerin, C., & American Forces Press Service. (2010, October 19). *Lynn: cyberspace is new domain of warfare.* Retrieved June 4, 2021, from U.S. Central Command: https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/884164/lynn-cyberspace-is-new-domain-of-warfare/

Reuter, C. (2015, April 18). *Secret Files Reveal the Structure of Islamic State*. Retrieved June 7, 2021, from SPIEGEL International: https://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html

Reuters Staff; Islamic State calls for attacks on the West during Ramadan in audio message. (2016, May 21). *Islamic State calls for attacks on the West during Ramadan in audio message*. Retrieved June 7, 2021, from Reuters: https://www.reuters.com/article/us-mideast-crisis-islamicstate-idUKKCN0YC0OG

Roberts, J. (2016). *Writing for Strategic Communication Industries.* Ohio: Ohio State University Libraries.

Roggio, B. (2014, January 4). *Al Qaeda, tribal allies 'control' Fallujah | FDD's Long War Journal*. Retrieved June 7, 2021, from FDD's Long War Journal: https://www.longwarjournal.org/archives/2014/01/al_qaeda_tribal_alli.php

Rona, T. (1976). *Weapon Systems and Information War.* Washington DC.: Office of the Secretary of Defence. Retrieved June 3, 2021, from https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf

Royo-Vela, M., & McBee, K. (2020). Is IS Online Chatter Just Noise?: An Analysis of the Islamic State Strategic Communications. *International Journal of Strategic Communication, 14*(3), 179-202. doi:10.1080/1553118X.2020.1770768

Schneider, N. (2015). *ISIS and Social Media: The Combatant Commander's Guide to Countering ISIS's Social Media Campaign.* Newport, RI: US Naval War College, Joint Military Operations Department.

Shabi, R. (2015, July 3). *Looted in Syria – and sold in London: the British antiques shops dealing in artefacts smuggled by Isis; the Guardian*. Retrieved June 8, 2021, from the Guardian: http://www.theguardian.com/world/2015/jul/03/antiquities-looted-by-isis-end-up-in-london-shops

Shakarian, P. (2021). Stuxnet: Cyberwar Revolution in Military Affairs. *Small Wars Journal, 23*, 1-10. Retrieved from https://smallwarsjournal.com/jrnl/art/stuxnet-cyberwar-revolution-in-military-affairs

Shakarian, P., Ruef, A., & Shakarian, J. (2013). *Introduction to cyber-warfare a multidisciplinary approach.* Amsterdam: Morgan Kaufmann Publishers, an imprint of Elsevier.

Shamah, D. (2014, September 21). *Video games, Twitter tricks: How ISIS pulls in the kids*. Retrieved June 7, 2021, from The Times of Israel: http://www.timesofisrael.com/video-games-twitter-tricks-how-isis-pulls-in-the-kids-2/

Shehabat, A., & Mitew, T. (2018). Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism, 12*(1), 81-99. Retrieved from https://www.jstor.org/stable/26343748

Siboni, G., & Koren, T. (2015). The Islamic State's strategy in cyberspace. *Military and Strategic Affairs, 7*(1), 127-144.

Siebert, J., von Winterfeldt, D., & John, R. (2016). Identifying and Structuring the Objectives of the Islamic State of Iraq and the Levant (ISIL) and Its Followers. *Decision Analysis, 13*(1), 26-50. doi:10.1287/deca.2015.0324

Sims, A. (2018). The Rising Drone Threat from Terrorists. *Georgetown Journal of International Affairs, 19*, 97-107.

Sisk, R. (2017, January 11). *More ISIS Drones Brought Down in Fight for Mosul: Military.com*. Retrieved June 7, 2021, from Military.com: https://www.military.com/daily-news/2017/01/11/more-isis-drones-brought-down-fight-mosul.html

Smith, T. (2017). The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare. *American Intelligence Journal, 34*(1), 54-58. Retrieved from https://www.jstor.org/stable/26497117

Solomon, E., & Jones, S. (2015, December 14). *Isis Inc: Loot and taxes keep jihadi economy churning; Financial Times*. Retrieved June 8, 2021, from Financial Times: https://www.ft.com/content/aee89a00-9ff1-11e5-beba-5e33e2b79e46

Solomon, E., Chazan, G., & Jones, S. (2015, October 14). *Isis Inc: how oil fuels the jihadi terrorists: Financial Times*. Retrieved June 8, 2021, from Financial Times: https://www.ft.com/content/b8234932-719b-11e5-ad6d-f4ed76f0900a

Solomon, E., Kwong, R., & Bernard, S. (2016, February 29). *Syria oil map: the journey of a barrel of Isis oil; Financial Times*. Retrieved May 26, 2021, from Financial Times: https://ig.ft.com/sites/2015/isis-oil/

Speckhard, A., & Yayla, A. (2017). The ISIS Emni: Origins and Inner Workings of ISIS's Intelligence Apparatus. *Perspectives on Terrorism, 11*(1), 2-16. Retrieved from https://www.jstor.org/stable/26297733

Stephens, M. L. (2020). Cats Turn the Tide of the Battle of Pelusium. *Aisthesis, Stanford Undergraduate Classics Journal, 3*(Summer 2020), 41. Retrieved from https://classics.stanford.edu/sites/g/files/sbiybj10936/f/publications/aisthesis_2020.pdf#page=47

Struble, D. (1995). What Is Command and Control Warfare? *Naval War College Review, 48*(3), 89-98. Retrieved June 4, 2021, from https://digital-commons.usnwc.edu/nwc-review/vol48/iss3/9

Sune Engel Rasmussen, U.-L. C., & Rasmussen, S. (2019, March 23). *U.S.-Led Coalition Captures Last ISIS Bastion in Syria, Ending Caliphate*. Retrieved June 7, 2021, from Wall Street Journal: https://www.wsj.com/articles/u-s-backed-force-says-islamic-states-caliphate-destroyed-in-syria-11553322489

Swanson, A. (2015, November 18). *How the Islamic State makes its money: Washington Post*. Retrieved June 8, 2021, from Washington Post: https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money/

Taschler, J. (2016, January 13). *Will ISIS Turn to Cyber Warfare?* Retrieved June 7, 2021, from Government Technology: Cybersecurity: https://www.govtech.com/security/Will-ISIS-Turn-to-Cyber-Warfare.html

The Independent. (2014, November 4). *The American prison that became the birthplace of Isis*. Retrieved June 7, 2021, from The Independent: https://www.independent.co.uk/news/world/middle-east/camp-bucca-us-prison-became-birthplace-isis-9838905.html

The Jerusalem Post. (2015, April 13). *ISIS hacks Australian airport website with threatening message to Israel*. Retrieved June 7, 2021, from The Jerusalem Post | JPost.com: https://www.jpost.com/middle-east/isis-hacks-australian-airport-website-396925

The United States Department of Justice, Office of Public Affairs. (2015, October 15). *ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges*. Retrieved June 7, 2021, from The United States Department of Justice: https://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges

Tønnessen, T. (2015, July 21). Heirs of Zarqawi or Saddam? The relationship between al-Qaida in Iraq and the Islamic State. *Perspectives on Terrorism, 9*(4), 48-60. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/443

U.S. Department of The Treasury. (2014, October 10). *Remarks of Under Secretary for Terrorism and Financial Intelligence David S. Cohen at The Carnegie Endowment For International Peace, "Attacking ISIL's Financial Foundation": U.S. Department of The Treasury Press Center*. Retrieved June 8, 2021, from U.S. Department of The Treasury Press Center: https://www.treasury.gov/press-center/press-releases/pages/jl2672.aspx

United States Department of State, About Us – The Global Coalition To Defeat ISIS. (2014, September 10). *About Us – The Global Coalition To Defeat ISIS.* Retrieved June 7, 2021, from United States Department of State: https://www.state.gov/about-us-the-global-coalition-to-defeat-isis/

Watson, B. (2017, January 12). *The Drones of ISIS*. Retrieved June 7, 2021, from Defence One: https://www.defenseone.com/technology/2017/01/drones-isis/134542/

Weiss, M., & Hassan, H. (2016). *Işid: terör ordusunun içyüzü* (1st ed. ed.). (E. Kayhan, Trans.) İstanbul: Kırmızı Yayınları.

Welch, T. (2018). Theology, heroism, justice, and fear: an analysis of ISIS propaganda magazines Dabiq and Rumiyah. *Dynamics of Asymmetric Conflict, 11*(3), 186-198.

Wood, G. (2015, February 16). *What ISIS Really Wants*. Retrieved June 6, 2021, from The Atlantic: https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/

Yarchi, M. (2019). ISIS's media strategy as image warfare: Strategic messaging over time and across platforms. *Communication and the Public; SAGE Journals, 4*(1), 53-67.

Zaman Al Wasl. (2017, February 19). *New ISIS document reveals group's electronic warfare projects.* Retrieved June 7, 2021, from Zaman Al Wasl: https://en.zamanalwsl.net/news/article/23528/