T.C.
HASAN KALYONCU ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

CYBERACTIVISM IN SYRIA
EMERGENCE, TRANSFORMATION, POTENTIALS AND LIMITATIONS

Iyad HELWANI

YÜKSEK LİSANS TEZİ

Gaziantep - 2024

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÜKSEK LİSANS TEZ KABUL VE ONAY FORMU

Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı Yüksek Lisans Programı öğrencisi Omar Garebo tarafından hazırlanan **"Cyberactivism in Syria; Emergence, Transformation, Potentials and Limitations"** başlıklı tez, **15/4/2024** tarihinde yapılan savunma sınavı sonucu **başarılı** bulunarak jürimiz tarafından **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Görevi	Unvanı, Adı ve Soyadı	Kurumu/Üniversitesi	İmzası:
Tez Danışmanı	Doç. Dr. Murat ASLAN	Siy.Bil. ve Uluslararası İlişkiler Bölümü/Hasan Kalyoncu Üniversitesi	
Jüri Başkanı	Doç. Dr. Mesut ŞÖHRET	Uluslararası İlişkiler Böl/Gaziantep Üniversitesi	
Jüri Üyesi	Dr. Öğr. Üyesi Pelin ALİYEV	Siy.Bil. ve Uluslararası İlişkiler Bölümü/Hasan Kalyoncu Üniversitesi	

Bu tez Enstitü Yönetim Kurulunca belirlenen yukarıdaki jüri üyeleri tarafından uygun görülmüş ve Enstitü Yönetim Kurulu kararı ile onaylanmıştır.

Doç. Dr. Ufuk AKBAŞ
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

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

Iyad HELWANI

09/01/2024

HASAN KALYONCU UNIVERSITY
GRADUATE EDUCATION INSTITUTE
DEPARTMENT OF POLITICAL SCIENCE AND INTERNATIONAL RELATIONS

CYBERACTIVISM IN SYRIA
EMERGENCE, TRANSFORMATION, POTENTIALS AND LIMITATIONS

Iyad HELWANI

MASTER THESIS

Advisor
Assoc. Prof. Dr. Murat ASLAN

ABSTRACT

The emergence of the cyber domain and social media platforms has revolutionized the socio-political landscape, especially in the Middle East and the Arab countries. It provided a platform for dissent, advocacy, and communication amidst protracted conflicts with authoritarian regimes and silencing voices of people. Cyber-activism has become a powerful tool for grassroots movements to reach a broader audience, mobilize support, and effect change. However, it faces challenges such as misinformation, censorship, and counter-activism. This research examines the role of cyber-activism in the Syrian context, focusing on its evolution, impact, challenges, and potential implications for future social movements. It also demystifies the trajectory of cyber-activism in Syria and helps to understand the circumstances surrounding the outcomes of cyber activists. The study employs a qualitative approach, integrating data gathered from professional reports, interviews with Syrian cyber-activists and cyber experts, and a scholarly literature review. The research delves into how online platforms have facilitated the mobilization, coordination, and dissemination of information among Syrian activists. Additionally, it investigates the challenges and risks cyber-activists face, including surveillance, censorship, security concerns, and cyberattacks. Also, this study explains the dynamics of cyber-activism within a heavily monitored and state-governed domain. The findings highlight the multifaceted nature of cyber-activism in Syria and its impact on shaping narratives, fostering solidarity, impacting the authoritarian regime, and influencing international perceptions. Ultimately, this study contributes to a more profound understanding of the complex dynamics of cyber-activism within the Syrian context. It sheds light on the transformative potential of digital platforms in amplifying voices, shaping narratives, fostering solidarity, and advocating for change in repressive environments.

Keywords: Cyberactivism, hacktivist, Syria, cyber conflict, Arap spring.

ACKNOWLEDGMENT

First, I would like to express my deepest gratitude to my supervisor, **Prof. Murat Aslan**, for his invaluable guidance, and constructive feedback throughout my master's research. His expertise, patience, and encouragement have been instrumental in shaping this thesis and enhancing my academic journey.

I would also like to extend my heartfelt appreciation to my wife, Ahd. Her understanding, and encouragement have been my source of strength and inspiration. Her unwavering belief in me, even during the most challenging times, has been pivotal in reaching this significant milestone.

Finally, and most crucially, I dedicate this work to the unwavering champions of justice and freedom. In particular, I honor the memory of the brave friend **Homam Hawasli**, whose cyber efforts in the pursuit of truth and liberty will forever be cherished and remembered, may God Almighty have mercy and blessings upon him.

Iyad HELWANI

Gaziantep - 2024

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
AP	Associated Press
APT	Advanced Persistent Threats
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
EU	European Union
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information And Communication Technology
ID	Identification
IP	Internet Protocol (IP) Address
ISP	Internet Service Provider
IT	Information Technology
MoCT	Ministry Of Communications and Technology
MSC	Mobile Switch Centre
NANS	National Agency for Network Services
NATO	North Atlantic Treaty Organization
NES	North East Syria
NGO	Non-Governmental Organization
NWS	North West Syria
PC	Personal Computer
RAT	Remote Access Tools
SCS	Syrian Computer Society
SEA	Syrian Electronic Army
SIM	Subscriber Identity Module
SMS	Short Message Service
SMT	Syrian Malware Team
STE	Syrian Telecommunication Establishment
SyTRA	Syrian Telecommunication Regulatory Authority

UAE	United Arab Emirates
UN	United Nations
URL	Uniform Resource Locator
US	United States
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

CHAPTER I

1. INTRODUCTION

1.1. Introduction

"Where is the Blue device ...?!!" An intelligence officer asked the Internet café owner after raiding his shop. The terrified café owner did not know what the officer wanted. Within seconds, intelligence personnel spread out in the café and started searching for the blue device. "They are using it against the government, they want to destroy the country"; the officer explained about the 'blue device' which protestors use to coordinate their demonstrations and communicate with the forces conspiring against the Syrian state. The café owner was lucky that the patrol that raided the café did not find such a device in his shop. The next day, the patrol confiscated the computers after they were shown that the blue device, they were ordered to get was something on the computer screen! The café owner then understood that they were looking for Facebook!

This was one of many stories that went viral after the outbreak of peaceful demonstrations in Syria in March 2011, which shed light on a new battle domain between the Syrian authoritarian regime and the activists.

The day the Baath party seized power in Syria in 1963, the ruling party enacted the Emergency Law. This law resulted in the restriction of certain rights that were promised in the Syrian Constitution, such as the freedom to gather, express opinions, and freedom of mobility for people. The law allowed the Syrian authorities to imprison individuals without any explanation or justification, and without offering them an opportunity to get proper legal processes and representation. Also, it allows regime agents to monitor people's actions. With the tight security grip imposed by the regime, people circulated phrases such as "Walls have ears," which refers to the regime eavesdropping on any conversation between two people, as well as to the self-censorship that people imposed on themselves for fear of being arrested. Syria became known as the Kingdom of Silence.

With the introduction of the Internet to Syria in the early 2000s and its limited spread after 2005, websites and social media platforms facilitated the creation and spread of content. This development had reflections on the social life of Syrian people as they felt that they had a new field away from the eyes of censors for expressing themselves,

exchanging information, and sharing ideas. They started to read freely; some dared to write and publish after years of deprivation and prevention.

Not long before, stories of arrests began for writing articles and publishing them on the Internet. However, the regime also started imposing severe censorship by blocking many websites, restricting entering Internet cafes, and spreading a state of surveillance on the cyber sphere.

With the outbreak of protests in March 2011, the Cyber domain was one of the main fields used in coordination, mobilization, awareness raising, and delegitimizing the Syrian regime. Internet use increased from about 5% of the population in 2005 to approximately 20% in 2012. The Syrian Revolution was described as the most documented crisis in history as it utilized the cyberspace capabilities to break the silence and disseminate media, including videos, photos, and live streaming of the movement and the repression that took place by the regime. This activism has become known as cyber-activism.

1.2. Research background

Cyber-activism significantly impacted the spread of the revolutionary movement during what is known as the Arab Spring. It has provided solid opportunities and a basis for political change but faced many challenges and notable limitations. In Syria, the authoritarian regime did not stand by and watch attempts by cyber activists to control this field. Instead, it was working diligently to make it also a monitored domain by first controlling the infrastructure and the installation of surveillance systems, then imposing laws that limit freedom of use, and finally deploying trained cyber groups to combat cyber activists in all aspects.

The Syrian regime followed a different policy from the policy adopted by the Egyptian and Libyan regimes, which was based on restricting Internet access to hinder popular movement and prevent it from spreading. The policy included lifting the block on most social media websites at the beginning of the events, as well as lifting the emergency law, which led to a direct increase in the number of users of social networking sites. For example, Facebook users increased from 1.5% of the total Syrian population at the beginning of 2011 to 10% at the beginning of 2012. On the other hand, the regime was brutally repressing the demonstrations with the absence of foreign news agencies and free press. Social media websites have become the only medium for documenting

violations and broadcasting daily events globally. This turned cyberspace in Syria into a conflict arena and made cyber-activism a case study for the use of cyberspace in authoritarian states such as the Syrian regime.

1.3. Problem Statement

The use of cyberspace as a field of activity in the Syrian social and political scene embodies a contradictory environment. While cyber activism offers a means for dissenting voices to amplify their narratives, mobilize support, and challenge the status quo, it simultaneously faces multifaceted challenges within the framework of authoritarian regimes. This research aims to carefully dissect the complex dynamics underpinning this dichotomy, examining the multiple constraints, risks, and ethical dilemmas faced by activists engaged in online dissent within an oppressive regime.

The primary focus is to understand the profound obstacles that online activists face, which include multi-layered government censorship, strict surveillance measures, and the threat of arbitrary arrest or kidnapping. Furthermore, the deployment of state-backed cyber groups and the potential for digital spaces to be weaponized further exacerbates the landscape, sowing seeds of confusion and fear of hacking and data theft within the activist community.

This study intends to explore the intricate relationship between the possibility of using cyberspace to change the political system and the substantial limitations due to counter-activism in Syria. By investigating these contrasting elements, this research aims to provide an understanding of both the benefits and opportunities as well as obstacles and limitations of utilizing cyber tools to drive social and political change in a country marked by strict control, censorship, and dictatorship rules.

1.4. Research Questions

The research questions were shaped by closely analysing cyber-activism in Syria since 2011 and examining the global reflection of the conflict in the cyber domain. The focus on understanding cyberspace's structure led this research to craft specific questions to guide the research and writing process. This approach helps us avoid creating a general overview and instead aims to support a specific and debatable aspect within our work.

Main Question:

- How can we understand the cyber-activism under the authoritarian regime in Syria?

  Sub Questions:
- What is cyber-activism? What are its characteristics, tools, opportunities, and impacts?
- How can cyberspace in Syria be described in terms of infrastructure, security, and communication?
- How does the authoritarian regime deal with cyberspace?
- What tools did the regime use to manage and control?
- From a security and intelligence perspective, how does the regime control and oversee activities in cyberspace?
- What are the main political activities in cyberspace in Syria before 2011? Who are the activists? What activities did they do? What was the impact?
- How did the Syrian regime deal with these activities?
- After 2011, what are the main characteristics of political activism in cyberspace, and how do they collect and manage their activities?
- How has cyber activism transformed during the different phases of the Syrian crisis?
- How did the regime manage cyberspace during the conflict?
- How did activists get rid of the restrictions imposed by the regime?
- What are the activities conducted in cyberspace in Syria during the conflict? Did these activities affect the authoritarian regime? How did it affect the authoritarian regime? Who are the main actors?
- How did these activities support field activities against authoritarian regimes?
- What was the international community's response to the regime and opposition in the cyber domain? What is the cyber operations impact on the international relations of authoritarian regimes? How did these operations change the regime's behaviour?

Answering these questions provides a comprehensive and detailed exploration of cyber-activism under the authoritarian regime in Syria. They are systematically structured to cover various dimensions, from defining cyber-activism and understanding the technical aspects of cyberspace in Syria to examining the strategies and responses of the authoritarian regime. The questions also effectively trace the evolution of cyber-activism before and after the onset of the Syrian crisis, highlighting key actors, activities, and

impacts. Additionally, they delve into the international dimension of cyber-activism, exploring the responses of the international community to cyber-activists.

1.5. Research Objectives

This research aims to delve into the world of cyber-activism in Syria, distinct from cyber warfare, to understand its power as a tool for political change during various phases of conflict. Central to this investigation is an exploration of how the Syrian regime has constructed and implemented a cyber surveillance system, and the subsequent impact of this system on the efficiency and efficacy of cyber-activism within the country.

The objective of this research is as follows:

- Understanding cyber-activism and how we can differentiate it from cyber warfare, its potentials, and limitations during different phases of conflict.
- Building knowledge on cyber activism as a means of political change.
- Understanding how the Syrian regime built the cyber surveillance system and how this affected cyber-activism efficiency.

Substantially, this study seeks to build a comprehensive knowledge base on cyber-activism, shedding light on its dynamics, challenges, and implications in the context of authoritarian governance and political resistance in Syria.

1.6. Research Hypotheses

Research hypotheses were proposed based on extensive reading of research conducted on the same issue, whether in Syria or similar countries. Although there is a limitation in finding a helpful number of references that describe cyber activities and cyber domains in Syria, this research is committed to employing the experience of the author in the information and communication field as well as in cyber-activism. The participation in Syrian activity after 2011 matched the practical experience of the author with the theoretical analysis presented in other research and extracted this into three hypotheses that were allocated within a purely scientific research framework to be of analytical and inferential value.

Consistently, this paper focus on cyber-activism under the authoritarian regime in Syria, and the literature review mainly focuses on understanding cyber-activism and providing a theoretical framework of the concept. Since the discussion revolves around

the role played by cyber-activism during the crisis, the dependent variable is the effectiveness of cyber-activism in political change in the repressive environment. On the other hand, there are multiple independent variables, namely the structure of the communications sector and cyber domain management in Syria, cyber activists' capacity level, access to the Internet, and the influence of cyber activity in the local community.

This thesis argues that cyberspace constituted the incubator of political activism under the strict security grip of the authoritarian regime in Syria. It provided the basis for the uprising to ignite, develop, and intensify over relatively short periods. It was less affected by the ideological transformation that affected the activists in other domains. On the other hand, the regime implemented a multi-layer surveillance methodology to hinder cyber-activism, and the limited development of network-related services in Syria reflected in the lack of targets that harm the government in cyberspace and consequently made cyber-activism in Syria less effective than other countries in the world.

Considering the elements discussed earlier and reviewing the research questions, sub-questions, and relevant literature, our research yields three hypotheses:

Hypothesis 1: The cyberspace in Syria is heavily monitored. The Syrian regime implemented a surveillance system in coordination with international ICT service providers.

Hypothesis 2: Cyber-activism in Syria played a cornerstone role during the uprising. It caused confusion and embarrassment to the regime in dealing with the movement and succeeded in achieving some objectives. However, hacktivists' operations were limited and lacked organization and leadership. Cyber-activism had almost reached a dead point by 2015.

Hypothesis 3: The international response to Syrian cyber-activists in cyberspace was minimal.

1.7. Significance of the Study

It has become known that the Arab Spring benefited from the development and spread of the Internet and social media. Cyberspace formed the appropriate space for activists to gather, coordinate, and freely express their opinions away from the eyes of censorship, as well as openness and communication with other cultures. After the outbreak of the revolutions in Tunisia, Egypt, and Libya, the wave reached Syria in March 2011. There were several attempts by different activist groups announced on different

social media networks before this date to assemble through social networks. Still, they were unsuccessful, and no studies explained why.

During the civil movement after March 2011, the so-called ‘coordination units’ were known in almost all of Syria. These ‘coordination units’ were working groups that mainly led to the documentation and dissemination of information about civil protests using cyberspace. Each of these coordination groups has a page on social media platforms for documenting and sharing the events and a virtual private group on the same medium to coordinate in a closed and secret manner.

Available research on cyber-activism in Syria focuses on cyber-attacks and non-state actors, such as the Syrian Electronic Army, during the conflict. They also study the tools they used, their efficiency, and how the regime reacted to this. However, cyber activities in Syria have not been studied as a means of political change, how the cyber-activists emerged and coordinated, what characteristics define the domain they were interacting with, how the regime prepared for this activism, and how they responded during the crisis. Moreover, none of the studies describes the domain in which the actors interact.

This research attempts to fill this gap, as it draws an integrated picture of cyber activity in Syria in terms of its emergence, the opportunities it provided, the challenges it faced, the international response and support, and how the regime interacted with it. Furthermore, it sheds light on international companies and countries involved in the cyber-crisis in Syria.

CHAPTER II

2. LITERATURE REVIEW: KEY CONCEPTS AND DEBATES RELATED TO CYBER-ACTIVISM

2.1. Definitions

When the term ‘cyber-activism’ is mentioned, the first thing that comes to mind is Facebook or Twitter (newly known as X platform) and the use of social media networks in political activities and campaigns. More technical-savvy people may think of cybersecurity and hacking operations, and others may talk about cyber warfare and the cyber-attacks that the news talks about from time to time between countries and espionage attempts and the disruption and blockade in countries' infrastructure.

This chapter outlines the general framework in which we conducted this research by presenting the most prominent definitions associated with the concept of “Cyber-activism” and building a foundation for understanding all the related terms.

The term “cyber-activism” comes from two main parts: the cyber domain or cyberspace, which includes the Internet and communications networks as a vital and modern field of communication. The second is activism, which describes any human activity, whether individual or collective, formal or informal, aiming to improve people's lives. This includes social, political, economic, or environmental reform. This can involve extreme action or participation, such as demonstrations or protests, to achieve certain goals or raise awareness about specific issues (Göksun, 2014)

While the internet is known as a network of networks, which means it is a global network formed by connecting smaller networks of computers and servers, it has become an unclear concept. When we talk about the Internet or the cyber domain, our focus goes beyond the technical aspects of the computer network to include its social fabric and contextual effects. Currently, questions regarding users, their intended purposes, and accompanying regulations and facilities are actively addressed by advertisers, businesses, government bodies, and civil society organizations. (Khamis & Vaughn, 2011).

Cyberspace, or as it will be used in this study, cyber domain, is merely a figurative and symbolic space that exists within the context of the Internet. It may be stated that anything done through the Internet occurs within cyberspace, whether sending an e-mail, creating a website, playing a game, or even shopping on e-commerce websites. In other

words, the cyber domain is the virtual space encompassing all interactions that rely on information and communication technology (ICT). Building on this, the cyber domain can also be considered a new domain of political interaction and a central information resource. As Neumayer and Raffi explained, “Blogs, Wikis, and social networking sites provide a technological basis for grassroots action to coordinate and for activists to communicate. Chat rooms, email, and mobile gadgets enable ad-hoc activities to emerge. The Internet can support the organization of topic-oriented pressure groups, protest organizations, and ideological movements outside the mainstream”(Neumayer & Raffl, 2008).

Researchers who discuss the concept of cyber-activism have put forward many definitions for this term. Some gave a general and simple description, such as 'tech-based activism’ or ‘politically motivated movements relying on the Internet’ (McCaughey & Ayers, 2003).

Others specified it, separated it from field activity, and restricted its use if offline field activity faltered, as Howard mentioned, "the act of using the Internet to advance a political cause that is difficult to advance offline”. (Kharroub, 2015) define it as the use of social media platforms to attain political goals in the realm of socio-political transformation.

Simply and building on all the definitions, we can say that cyber-activism is taking advantage of the cyber domain to achieve a specific cause. This cause may have an actual presence in the field, and cyber-activism supports it, or the use of the cyber domain was due to the difficulties or potential threats to carrying out this cause in the field. This cause may be a humanitarian, political, economic, or social activity. This may be by using social media networks to raise awareness and mobilize or by carrying out cyber operations such as hacking websites or other cyber-based tools to achieve the cause's goals.

Cyber-activism is distinct from cyberwarfare, as it is typically neither initiated by a state nor recognized as war by the international community. It is usually a group of actions by individuals or groups affiliated with social movements, prioritizing information access, capitalizing on the internet's networked nature, and leveraging digital media and social platforms to foster socio-political transformation and amplify collective voices. Furthermore, it is distinguished from cyberterrorism, which is defined by NATO as “using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or intimidate a society into an ideological

goal”(Mehan, 2015). Cyber-activism mainly concerns changing the current status quo and motivating people to achieve the cause.

2.2. Cyber-activist, Hacktivist Cybercriminal, and Cyberterrorist

Many terms are synonyms for cyber-activism, including digital activism, online activism, internet activism, and hacktivism (Hennefer, 2013). However, the term ‘Hacktivism’ refers to a specific category of activists known as Hacktivists. Hacktivists aim to achieve broad political influence by targeting particular organizations or sources of information. Although cyber-attacks have existed since the beginning of the Internet, their importance increased dramatically in 2011, during which attempts at change exploded in the Arab world. According to Verizon's report on data breaches, cyberattacks by hacktivists accounted for 100 million of the 174 million attacks recorded in 2011. (Mehan, 2015).

Accordingly, we can define hacktivism as committing cyberattacks, especially hacking, to achieve a cause's goals, which may often be political or related to human rights. It has also been known as political hacking (Applegate, 2011). Thus, by this definition, Hacktivism is within the umbrella of cyber-activism.

Cyber activists differentiate themselves from cyber criminals as the latter carry out cyber-attacks to achieve financial gain, and from cyber terrorists in that the cyber operations they carry out do not lead to acts of violence, harm, or loss in the lives of others, even the opponents.

Considering that we mentioned cyber operations here, it is good to explain that we mean by these operations that the objective is to accomplish strategic goals or create impacts within or through cyberspace and to use cyberspace capabilities (Sigholm, 2013). It mainly includes using cyber espionage, hacking, denial of service, advanced persistent threats, phishing, and malware, which we will explain in detail in the tools of cyber-activism section.

It is essential to highlight that engaging in a cyber cause does not necessarily consider cyber-activism. For instance, people aiming to support a social or political cause often engage with no effort, which saves time and money and minimizes any potential risk, such as pressing sharing or retweeting. These online activities boost the self-esteem of those involved yet reflect almost no impact on real-world causes. Consequently, the satisfaction derived from a mere click of a button coined as 'online activism' sometimes

overshadows the substantial implications of traditional activism, which has a demonstrated impact on fundamental societal changes. This kind of activity is called **slacktivism or clicktivism**, defined as "feel-good online activism that has zero political or social impact" (Kharroub, 2015). Examples include liking a Facebook post, upvoting on Reddit, retweeting on Twitter (X platform), changing a profile picture, and other everyday actions on social networking platforms (Hennefer, 2013).

2.3. Characteristics of Cyber-activism

One of the most prominent features of the information and telecommunication technology era is that it has fundamentally restructured social and political life. It provided structural opportunities, enabled tactical event engagement, and facilitated collective actions. An essential characteristic of using ICT in political participation is that it has provided almost free access, especially in terms of participation cost, and the ability to promote collective identity and form virtual communities that effectively reflect real life. For example, social networks enabled activists to communicate within a secure domain that helped them exchange ideas and discuss political concepts almost without cost compared to what would have happened in real life (Radsch, 2016). Cyberspace also provided the activists with a safe domain to break censorship on content and media imposed by authoritarian states, whether by accessing or publishing and sharing information (Göksun, 2014).

Another essential characteristic of cyber-activism is anonymous participation, which gives security to participants, whether simply writing and gathering or engaging in cyber-attacks without the ability of opponents to identify them (Applegate, 2011). This is one of the most prominent characteristics that facilitated revolutions in the Arab world and promoted its expansion under authoritarian regimes, especially in Syria, in which freedom of assembly and freedom of speech has been suppressed by the Emergency Law since 1963. For example, Syrians have been using fake names on Facebook to mobilize people for demonstrations and publicize the brutal oppression they were facing(Applegate, 2011).

Furthermore, cyber-activism allows people from different affiliations to engage together and have their voices heard by the rest of the communities (Göksun, 2014). Sighlom argued that the most present activists on the network are ordinary citizens (Sigholm, 2013). This was obvious during the first weeks of the Syrian uprising, where,

for almost the first occasion, various components of the Syrian community engaged in the multi-ethnic movement, including Arabs, Kurds, community leaders, youth, Islamists, Christians, communists, and exiled intellectuals within social media networks and became able to exchange opinions and express their views and ideas freely, after the authoritarian state altogether forbade it for decades (Khamis et al., 2012).

Free exchange of opinions and ideas between diverse groups in communities made resonant speeches and physical gatherings are no longer the sole means to garner support or promote an idea. Credibility is now linked to receiving likes, retweets, or followers—a shared validation or dismissal (Radsch, 2016).

Cyber-activism is unlikely to alone lead to, for example, political independence or the fall of ruling regimes. Likewise, cyberattacks are not considered an attack on the state under international law because an attack, according to international law, includes in its definition the term "violence against an opponent," and cyberattacks cannot be considered attacks that carry the character of acts of violence (Applegate, 2011).

Cyber-activism is characterized by accessibility as engagement in causes is affordable at almost no cost, the absence of communication barriers, and the ability to interact globally without constraints. It also provides the freedom to share and exchange ideas anonymously and safely. It breaks through censorship in information sharing, enabling marginalized groups to participate and express opinions freely and allowing for easy support or opposition of ideas without direct contact, without being construed as violent activity.

2.4. Types of Cyber Activism

Cyber-activists can carry out different types of activities within the cyber domain. These activities vary depending on the nature of the proposed action, the tools, and the objective. Some activities go under journalism, such as publishing news and articles, in which social media plays a significant role as a tool that allows instant news publishing within networks. Other activities are campaigns to pressure a specific party or awareness-raising and training activities to raise awareness of the use of the cyber domain and avoid censorship or cyber-attacks to take over specific information and embarrass the opposing party.

We can categorize the actions under the following groups:

- Citizen Journalism involves activists utilizing online social media platforms like Blog, Facebook, Twitter, and YouTube. They use these platforms to bring attention to government abuses against their citizens, advocate for political transformation, influence public perspectives, live-stream protests, and rally fellow citizens to resist oppression (Khamis et al., 2012).
- Online petitions, demonstrations, and campaigns: Internet platforms facilitate a range of actions like raising funds, creating international alliances, sharing petitions and alerts, and coordinating local or global events. This underscores how information and communication technology (ICT) transforms into a space where different viewpoints compete to shape people's thinking. These contrasting narratives aim to influence the opinions of specific audiences, underscoring the importance of this digital space in capturing people's attention and perspectives. (McCaughey & Ayers, 2003)
- Digital literacy and cybersecurity safety training: training in digital literacy and cybersecurity focuses on equipping activists with essential skills to safeguard themselves while operating online. It involves providing necessary tools and developing platforms that enable secure online activism, aligning with activists' goals. The significance of this training becomes evident in regimes that enforce strict censorship, leading to the arrest and torture of activists. It is also crucial in countries with limited technical expertise, where using the internet for cyber activities remains challenging.
- Cyber-attacks, often executed by hacktivists, involve targeting the websites or networked computers of governments, corporations, or entities that align with specific political viewpoints. The objective of these attacks is to establish influence by causing damage or infiltrating the information and communication systems of the opposition. The motives behind such actions vary—from expressing disapproval to raising public awareness (McCaughey & Ayers, 2003).

With no doubt, many other categories might be mentioned; for example, some resources split cyber-attacks into smaller groups, including denial of service attacks, data leaking and whistleblowing, and hacktivism. Furthermore, online campaigns also split into cyber protests and anonymous activism. However, each category shares the same tools and almost demands the same technical skills by the activist.

Based on the objective of online activism, Sander Vegh argues that cyber-activism falls into three general areas: awareness/advocacy, organization/mobilization, and action/reaction. (McCaughey & Ayers, 2003)

- Awareness/advocacy: disseminating information online using email lists, websites, or social media networks. The activist establishes networks for distribution, which can subsequently be utilized for organization and mobilization purposes. The presence of these networks proves to be very useful when the moment of political change comes. For example, “We are all Khaled Said” page on Facebook initiated the Egyptian revolution. The targeted audience can be either part of a specific group, such as parties or NGOs, informal collective, a lobbying organization or a civic movement. Another example is campaigns boycotting Israeli products, which formed around a particular issue and resulted in cyber lobbying.
- Organization/mobilization: Through online dissemination channels, activists can call for an offline action, such as a protest in a specific location and point of time. Also, it can be used to appeal online action, such as sending a letter to a UN agency through e-mail to put global pressure on an action or retweeting a US president's post to show an opposing opinion.
- Action/Reaction: Hacktivists usually have their online forums to call for collective cyber-attacks against specific targets, such as turning down vital websites and services through denial-of-service attacks, hijacking traffic to the official website by publishing cloned ones, or hacking websites and social media accounts to gain critical information.

In conclusion, the activities conducted by cyber-activists span diverse areas, from citizen journalism and online campaigns to digital literacy training and cyber-attacks. These categories highlight the pivotal role of ICT in facilitating various forms of online activism, including awareness-raising, mobilization, and direct action. On the the hand, Sander Vegh's framework further categorizes cyber-activism into awareness/advocacy, organization/mobilization, and action/reaction, emphasizing the dynamic interplay between information dissemination, mobilization, and cyber-attacks. Together, these frameworks provide valuable insights into the multifaceted strategies employed by cyber-activists in leveraging digital platforms for political change and resistance against oppressive regimes.

2.5. Tools of Cyber-Activism

Cyber-activism tools vary depending on the carried-out activity and the impact it aims to achieve. These tools range from communication platforms and social media networks to specialized software and techniques designed to enhance online security and anonymity. Understanding the diverse toolkit available to cyber-activists is crucial for comprehending the intricacies of digital activism and its potential to foster political change and resistance in the contemporary digital landscape. This section aims to explore the various tools employed by cyber-activists, highlighting their functionalities, applications, and significance in facilitating different forms of online activism and mobilization.

2.5.1. Social media networks and blogging

Social media platforms are considered the best tools for mobilization, awareness-raising, and advocacy in this field. Also, each social media platform has its features to use efficiently. Facebook is notably the best tool for communication and mobilization. Facebook indeed provides a platform for individuals to connect and communicate with others who share similar views and interests. It can also be used to mobilize individuals around a specific concern or cause to gain collective assistance and support. This was demonstrated in the case of "We are all Khaled Said", the most famous Facebook page in Egypt. It played a crucial part in increasing consciousness or promoting awareness about human rights violations and police brutality, mobilizing people, and motivating them to revolution in 2011.

While Twitter played a clear role in organizing crowds and coordinating in real-time, this was demonstrated in Tahrir Square in Egypt, as well as how to route the crowd and keep people updated about the best directions to avoid the police and reach the square (Khamis & Vaughn, 2012). Twitter was also an effective communication tool with foreign journalists (Radsch, 2016). Furthermore, Twitter allows the use of pseudo-names within its policy, unlike Facebook, which makes it considered better for activists who prefer anonymity.

The strict policy implemented by Facebook and the deletion of many accounts pushed many cyber-activists to use blogs. Many mentioned that Facebook turned into a closed, restricted sphere; no one can see your posts without group approval or being friends (Radsch, 2016). Blogging provides space for unrestricted self-expression and free

writing. Activists can break political and social taboos and write about public issues, such as government corruption and human rights violations, which helped raise awareness and facilitated the outbreak of protests in many countries (Khamis, 2017).

In countries where authoritarian regimes ultimately control media, YouTube and other video streaming tools have become essential for broadcasting live protests, enabling real-time dissemination, and documenting protests and violations that might have otherwise remained hidden from public view. A clear example of this is citizen journalists who documented the atrocities during the Syrian uprising. Cyber-activists put themselves at risk by filming these events, smuggling the recordings out of the country, and sharing them on YouTube. This act informed audiences worldwide about the tragedy in Syria, circumventing the government's restrictions on foreign correspondents and international media personnel (Khamis, 2017).

Many other online applications can play an important role in activism when cyber-activists utilize them effectively. Google Maps served as a crucial tool for informing protesters about the locations of gatherings and identifying areas where pro-government forces were present. International news agencies also employed this application to guide citizen journalists to optimal vantage points for reporting and coverage. Collaboration between news networks and civilian reporters provided a detailed and vivid portrayal of the atrocities. This coverage prompted people in the Western world to react by pressuring their governments to intervene in the violence through sanctions or military actions (Lee, n.d.). Skype, Telegram, and Signal applications were used to communicate, especially with news channels, as well as communication between activists on the ground in different regions, as secure communication channels that provide encrypted messaging. Governments have increasingly embraced the popularity of online petitions and surveys as practical tools for engaging with the public and gauging public opinion.

2.5.2. Cyber-attack tools

On the other hand, tools used in cyber-attacks are almost the same as the tools and methods used by cyber criminals who aim for profit. Although their objectives differ, hacktivists rely on 'Advanced Persistent Threats' or APTs for information exfiltration and cyber espionage. They secretly infiltrate an information system and create a method to return later and steal more data without being detected by the victim or causing any damage to the system (Mehan, 2015).

A commonly used method for cyberattacks involves the Distributed Denial of Service (DDoS) attack, where malicious actors attempt to disrupt online services by overwhelming them with a high volume of traffic. Within forums, hacktivists frequently exchange detailed instructions, lists of targets, and tools, sharing these resources openly. The result of these attacks is paralyzing the services and causing a mess in attacked party systems. In February 2013, American Express became a target of a distributed denial of service (DDoS) attack, making their website inaccessible for several hours. Izz-Eddin al-Qassam claimed responsibility for these attacks, citing retaliation against an anti-Islam video (Mehan, 2015).

Among the most advanced types of attacks is the Malware attack. This type of attack entails using malevolent software to hack, harm, or gain access to computer systems or networks without authorization. Malware can come in different forms, including viruses, worms, Trojans, ransomware, spyware, and adware. These types of malwares can lead to various consequences, such as data loss, system damage, financial loss, or theft of personal information. Malware can infect systems through email attachments, infected websites, software vulnerabilities, and other means. An example of this attack is the use of the FinFisher spyware application by Egyptian police during the Egyptian Revolution to attack dissidents. It used Trojans known as Remote Access Tools or RATs. These trojans plant bugs on the victim's personal computer to have the ability to see emails, and conversations over chat applications, or even intercept Skype calls (John Leyden, 2011). This kind of attack was also widely used during the Syrian uprising, especially by hacktivist groups and government-allied non-state actors.

One last cyber-attack to explain is phishing. Phishing is a deceptive cyber-attack method wherein perpetrators send emails or messages posing as reliable sources to deceive individuals into divulging sensitive information. These tactics frequently leverage urgency or fear to push recipients to click links or disclose personal details. In Syria, pro-government non-state actors employed such attacks by spreading fake news like ‘breaking exclusive news.’ Then, after clicking the link, it displays a fake login on Facebook, which requests users to log in again, enabling them to steal user credentials. (Clinic et al., 2021)

2.5.3. Internet access and safety tools

In many authoritarian regimes, governments enforce complete internet shutdowns in conflict-ridden areas, a tactic witnessed in certain Syrian regions like Daraa, Homs,

and the Damascus countryside. This strategy aims to disrupt internal coordination among activists across different areas and to prevent communication with international news outlets. Additionally, governments block numerous websites extensively utilized by cyber activists for mobilization and organization, as seen during Egypt's revolution. Severe censorship exists in both Egypt and Syria, exposing activists to risks of discovery, arrest, or even harm due to their online presence.

This situation compelled cyber activists to seek alternative means of internet access. In Syria, activists circumvented network outages by smuggling communication equipment and using SIM cards for networks in areas near the borders with Türkiye, Jordan, and Lebanon. Satellite internet modems and mobile phone SIM cards from neighbouring countries are smuggled as an alternative communication and internet solution to state-provided services.

Cyber activists resorted to using Anonymous Browsing Tools and Virtual Private Networks (VPNs) to secure access to blocked websites and social media networks. Anonymous browsing tools, like TOR, safeguard users' identities and locations by routing internet traffic through a global server network. VPNs encrypt internet connections, which is crucial for activists in regions with restricted internet access or surveillance.

2.6. Advantages, Opportunities, and Impact of Cyber-Activism

In authoritarian states, fear of arrest is considered the most significant obstacle to political participation and mobilization. However, the layout and functionalities of social media and Web 2.0 technologies enable ordinary individuals to assert their democratic rights and challenge states control over information. These digital platforms are instrumental in initiating, coordinating, mobilizing, and documenting events of activism. (Biswas & Sipes, 2014).

Cyberspace provided civilians, including minority groups, many opportunities to overcome fear, interact, speak up, mobilize, and organize collective actions safely and almost free of cost. Moreover, through hacktivism, activists could launch cyber-attacks and achieve impact without causing physical damage and with nearly no cost. By taking advantage of cyber-activism capabilities, activists have won global public nations ‘hearts and minds’ (Applegate, 2011). In Syria, for example, one of the essential opportunities attributed to cyberspace is providing the ability to communicate and share information for Syrian activists, as there is no opportunity to do this physically under a repressive

regime. According to a Syrian human rights activist: “The Internet is the only option for intellectuals to meet and share ideas” (Kharroub, 2015). This helped remind and disseminate information and keep the discussion on human rights violations alive.

Cyberspace and social media networks played a critical role in averting the immediate suppression of the revolution in Syria (Biswas & Sipes, 2014). Engaging in online communication with like-minded individuals has been linked to increased offline political participation(Biswas & Sipes, 2014). In Syria, widespread access to mobile information technologies and high levels of e-literacy among citizens and activists allowed unprecedented real-time access to ground events. The abundance of Syrian data largely stems from involved parties aiming to expose the severity of their brutality. This includes images of casualties and statements glorifying violent acts (Powers & O’Loughlin, 2015).

Cyber-activism encompasses two primary objectives: Firstly, it utilizes cyberspace to address issues originating from the offline realm. Civil society leverages cyberspace effectively for agenda setting, shaping public opinion, mobilizing the masses, and collective action to achieve their political aims. Cyberspace is harnessed as a potent tool to drive the goals of social movements. Secondly, it operates within cyberspace, aiming to resolve internal issues within this digital domain. Cyber-activism transformed into a movement rooted in cyberspace, striving to safeguard citizens' interests by circumventing limitations imposed on information transmission(Chang & Lee, 2006).

2.7. Limitation of Cyberactivism

Internet Access: Cyber-activism has indeed provided many opportunities for people to participate in change and break the media monopoly, as well as communicate and communicate their voice to the world, but that is not the case. For example, not all segments of the population can access the Internet, either due to a lack of infrastructure or low digital literacy (Neumayer & Raffl, 2008). Internet users are expected to be 66 percent of the global population by 2023 (cisco, 2020). These numbers are expected to be mostly in well-developed countries. For example, in Syria in 2014, total internet subscribers were around 5 million, comprising around 22% of the Syrian population (Göksun, 2014). Also, there is an access limitation due to age, as online activism is often more attractive to the youth than older people who have a weak ability to use it and see it as a passive method of participation (Hennefer, 2013).

Internet Surveillance: Furthermore, even among those with internet access, not everyone possesses the same opportunities or freedoms to express their opinions online, particularly in nations where governments implement firewalls and monitor online activities (McCaughey & Ayers, 2003). Authoritarian and oppressive regimes have also harnessed social media and the internet to identify and target activists (Kharroub, 2015). For example, in Syria, the government established a regulatory body overseen by intelligence apparatus that authorize citizens seeking to purchase a personal computer or modem or register as Internet users to obtain government approval (Göksun, 2014). On the other hand, major corporations own social media platforms and wield significant control over the content uploaded to these spaces, leading to ease in tracking and monitoring users (Mansour, n.d.). For instance, Facebook and YouTube were unblocked in February 2011, after being blocked for three years, coinciding the outbreak of anti-regime unrest. Unblocking Facebook and YouTube was perceived as an effort to monitor online activities by the Syrian regime while targeting and suppressing activists through these digital platforms (Kharroub, 2015).

Social Media Limitations: Social media usage often falls into two patterns as echo chambers, where users engage with like-minded individuals, and platforms for venting anger or attacking opposing views. This leads to extremes of an uninformed, emotionally driven consensus or aggressive divergence. These online spaces frequently lack the balanced middle ground of rational discussion and dialogue (Khamis, 2017) . Also, the impact of using social media in cyber-activism varies with the political environment. During unified moments like the Egyptian revolution in 2011, social platforms act as catalysts, amplifying voices and fostering unity for change. However, once unity wanes, these platforms can fuel divisions and polarization, as seen in countries in the aftermath of the Arab Spring Similar to Egypt's situation after June 2013 (Khamis, 2017).

Furthermore, Social media platforms, lacking clear hierarchies and prominent leadership, are often praised for enabling grassroots movements (Kharroub, 2015). However, this aspect might have contributed to the decline of post-revolutionary political movements. Social media alone cannot drive civic engagement or fill societal power gaps. In Arab Spring countries, the absence of an active civil society, structured opposition, and decentralized leadership created a vacuum that hindered democratic progress. While social media facilitated a favourable environment for change, it could not overcome the deficiencies impeding a smooth transition to democracy (Khamis, 2017).

Algorithmic censorship, observed in search algorithms and social media feeds, dictates what content gets prominence while suppressing others based on undisclosed criteria. This phenomenon, influenced by algorithmic personalization and collaborative filtering, might limit visibility, especially with evolving algorithms. For instance, A Syrian Facebook page, like "We are all Hamza Alkhateeb", faced closure and restoration by the platform, highlighting potential censorship concerns (Shehabat, 2013).

Citizen Journalism: Citizen journalists, due to their lack of professional training, require thorough fact-checking and verification before their reports can be fully trusted. Their content might contain inaccuracies, incompleteness, or even fabricated information, necessitating caution when consuming it online. Misinformation can be found in various media, including mainstream outlets. However, the risk tends to be higher in citizen journalism because of the absence of institutional structures, control mechanisms, professional standards, and formal journalistic training. (Khamis, 2017).

Lastly, using cyber-attacks in undeveloped countries that do not rely on information and communication technology as infrastructure and do not provide online services does not significantly impact achieving cyber-activism goals. For example, there is no e-government in Syria, and most governmental websites do not provide services but are merely news pages. Hacking operations on these sites were just a limited media battle, mobilizing people and exposing regime practices by publishing them on their websites.

CHAPTER III

3. METHODOLOGY

3.1. Scope of the Study

Cyberspace has become the cornerstone for many states in communication, military command and control, commerce, power plant distribution, transportation, and numerous critical infrastructures essential to enabling and sustaining modern society. In Syria, although some governmental institutes had access to the internet in 1996, the authoritarian regime did not allow citizens subscriptions until 2000. After 11 years, the widespread availability of the Internet formed the infrastructure to support and document the Syrian revolution against the regime through social networks and different cyber-activism platforms.

This research focuses on the emergence of cyber activism in Syria, understanding the opportunities and limitations, the structure of cyberspace, how it affected cyber-activism efficiency, and how the interaction between cyber conflict and on-ground conflict means the activists' impact on the authoritarian regime.

3.2. Research Design

To have diverse perspectives on cyber-activism, this research utilizes a mix of qualitative methodologies, including:

- The theoretical study will provide a broad background and understanding of cyber-activism amid ongoing discussions regarding Cyberactivism and cyberwarfare.
- Academic research and articles related to global cyber-activism and studies on cyber-activism in regions like Syria, such as Tunisia, Egypt, Yemen, and Libya.
- Official reports from reputable organizations, including research centres at universities, which carefully studied cyberspace in Syria through collecting valuable data and statistics from government agencies, policy analysis, and case studies.

Personal interviews with two groups of key informants: four cyber-activists and five Cyber experts. Two different tools were used to conduct semi-structured interviews.

To comprehend the experiences of activists in both online and offline realms and their utilization of information and communication technologies (ICTs), this study employed semi-structured interviews with four cyber-activists. The aim was to build knowledge of their cyber tactics, understanding of the cyber domain, and impact.

The interviewed cyber activists were involved entirely in internet activism, such as live streaming for protests, contacting international news agencies actively posting on social media about the situation in Syria during the uprising, and finding solutions to keep besieged areas connected to the internet. Five cyber experts included professionals working in communications and Internet services, including various companies and those working in the headquarters of these companies and fully informed of the decision-making mechanism. It included people working in Syriatel and MTN, the leading operators in Syria, and the Syrian Computer Society SCS-net.

3.3. Population and Sampling

This section presents detailed profiles of key informants involved in the Syrian cyber-activism landscape, offering firsthand perspectives on the strategies, challenges, and innovations driving digital activism in the country. From activists to ICT experts who were former employees of telecommunications companies, these interviewees provide valuable insights into the multifaceted nature of cyber-activism and the complex interplay between technology, activism, and governance in the context of Syria.

Below is a detailed description of the interviewees:

- Ahmad is a 35-year-old activist who has participated actively in many events and protests and has active accounts on Twitter and Facebook with thousands of followers. Ahmad was arrested many times by intelligence forces, and the last one was because they found a photo of a demonstration on his mobile phone while questioning him at a checkpoint near his house.
- Samer, a 44-year-old activist and ICT expert, was living outside Syria when the revolution started and was supporting activists via satellite internet before he returned to Syria. He spent a long period in a besieged region.
- Wafi, 33 years old, was another professional ICT expert who was a university student in computer science when the protests broke out. During the revolution's early days, a friend introduced Wafi to Samer, and then they initiated solutions for live streaming together.

- Abdulkadir, 38 years old, was involved in the revolution from the start and was a social media activist and blogger; he has many connections with cyber-activists and was participating in sharing video recordings of protests.
- Omar was an employee at Syriatel between 2010 and 2015. His role in human resources provided him with information on international experts supporting the company.
- Fatih was also an employee specializing in project management Syriatel from 2005 to 2012, and during his work, he had experience on
- Ziad, a 39-year-old professional computer engineer, worked in Syriatel between 2006 and 2012 in a sensitive position in the company headquarters. Ziad attended multiple meetings with Syriatel's former CEO, Rami Makhlouf – cousin of President Bashar Assad.
- Yusuf, a network engineer, worked for more than six years in MTN, the second mobile operator in Syria. Tamer was in direct contact with STE as he was responsible for maintaining and routing the telecommunication station.
- Kareem, a computer engineer, worked in operations at the SCS-net headquarters. Yusuf was responsible for monitoring network applications.

The insights shared by the interviewees highlight the resilience, innovation, and adaptability of cyber-activists in Syria. Their experiences, ranging from direct activism and technical support to roles within telecommunications companies, contribute to a comprehensive understanding of the challenges, strategies, and dynamics driving cyber-activism in the country.

3.4. Research Period

Cyber-activist groups were directly involved in Syria's cyber conflict between 2011 and 2016. This period was reported to be the peak in activism on the Internet and involved the highest number of cyber-attacks and operations.

On the other hand, the cyber experts worked in telecommunications companies in Syria between 2007 and 2014. In this period, the Syrian regime was building the surveillance system on the system and applied new methods such as tracking and censorship after the outbreak of protests in 2011 and then. Each interview lasted between 40 to 70 minutes.

3.5. Research Limits

The limitation of this research is that we could not include any state-backed cyber-activist from the Syrian Electronic Army or Intelligence forces. We tried to overcome this limitation by including studies covering this research area.

3.6. Data Collection

Before conducting the interviews, the researcher obtained informed consent from interviewees, and the interviews were recorded, except for one, as requested by the interviewee, who preferred not to record and accepted taking notes during the interview. Moreover, the researcher ensured confidentiality for interviewees and conducted the interviews via meeting software. The names used in this study are pseudo names and the descriptions used in this study ensured that it does not provide exact information so they cannot be identified.

3.7. Instrument

Two different semi-structured interview questions were used during the interviews. The interviews were held online using Zoom, and they were recorded. The interviews were structured around ten questions covering the main sections of this research. The questions are attached in the annex.

3.8. Data Analysis

The interviews were transcribed and analysed to identify common themes and patterns. Instead of real names, the researcher used pseudonyms for all interviewees to keep their privacy.

CHAPTER IV

4. CYBERSPACE LANDSCAPE IN SYRIA

4.1. Introduction

Global telecommunications technology has maximized the role of media, diversifying its functions in societies. Media witnessed a qualitative leap from its classic function of news transmission and event coverage to contributing to the reproduction of cultural heritage within societies and shaping public opinion. This evolution culminated in the concept of developmental media through the partnership between media and development, disseminating and ingraining universal human and civilizational values. The ease and speed of dissemination achieved by various media platforms increased the importance of this role. Compared to the number of radio users, Internet users reached 50 million users in less than four years, while radio took 38 years to reach the same number.

The internet arrived late in Syria, and until 1999, Syrian citizens were not allowed to subscribe to it. In the earliest independent report about the internet in Syria, Human Rights Watch stated: “Syria remains the only country connected to the internet in the region that has not yet allowed its citizens local access to the network, despite some official circles issuing statements extolling the advantages of the internet. This cautious approach by the government aligns with its efforts to restrain all forms of expression critical of the country's governance. However, some state institutions have had internet access since 1997, and there are reportedly a few thousand modem devices in Syria that, if accessible, allow registration with companies providing internet services in Lebanon and elsewhere.” (Scmadmin,2011).

It was evident in the "Kingdom of Silence," as it is called, that the Syrian regime saw the internet as a new space that allowed citizens to access information away from local media outlets that spoke only in the regime's name. Similarly, under the state of emergency law that prohibited any form of meetings or political discussions, the internet became a new space for people to connect away from the eyes of the authorities.

4.2. Cyberspace in Syria: Historical Context and Infrastructure

The Ba'ath Party, ruling in Syria, came to power in 1963. Emergency law granted the state control over all communication and media institutions, including broadcasting

entities, advertising agencies, newspapers, and magazines. The emergency law gave government agents the right to monitor their people and arrest them without even providing a reason. Individual liberties, including freedom of assembly, expression, and movement, were restricted by this law that granted the government extensive power to interrogate and detain individuals deemed to pose a threat to national security and public safety. This law also allowed for the detention of human rights defenders, journalists, and lawyers who opposed the Syrian regime without any legal justification beyond unspecified national security concerns. (Wilhelmsen, 2014)

After 1974, the role of Syrian media became centered on reinforcing dictatorship by broadcasting a singular discourse—the ruling party's message—and amplifying the image of the then-president Hafez al-Assad. No other component in society could access any media platform. During the 1990s, with the emergence of satellite channels and the internet, the Arab world witnessed a significant media transformation. However, Syria lagged all other Middle Eastern countries in granting access to the internet and marked to be the last one to do. This began in 1997 and was described by state institutions as cautious permission. At the time, the Minister of Communications described Syria's strategy in modern technologies, emphasizing that it wouldn't jeopardize its security and independence (Scmadmin,2011).

This security-focused strategy initiated a trial project for internet usage in 1996, officially starting in 1997, catering only to 150 subscribers from government or semi-governmental entities. The experimental project included a dedicated server to monitor the network and block undesirable websites. The objectives were to "train technical staff in monitoring, discovering, and blocking unwanted sites" and to "establish regulatory rules for extensive internet utilization." It gradually expanded until 2001 (Scmadmin,2011).

Bashar al-Assad took power in 2000, having previously held the position of head of the Syrian Computer Society (SCS), established by his brother Bassel al-Assad, leading it until he died in 1994. Among Bashar al-Assad's promises was to make the Internet available to Syrian citizens. Between 2001 and 2005, Syrians wishing to access the Internet had to submit an official request to one of the service providers operating in Syria, attach a copy of their ID, and await approval. Sometimes, citizens had to wait months to obtain subscription approval, often contingent on security clearance (Scmadmin,2011).

The percentage of people with internet access was estimated at 0.2% in 2000 and around 5% in 2005. This figure notably increased in the following years, reaching

approximately 20% by 2010 (Baiazy, n.d.). As of 2021, the estimated percentage of Syrian people with internet access is around 35% (Clinic et al., 2021).

4.3. Governmental Entities and Corporate Bodies

The management and control of the cyber domain in Syria is a little bit complicated as many bodies are interfering. both governmental entities and corporate bodies play crucial roles in shaping the digital landscape, from policy formulation and infrastructure development to innovation and digital services provision.

Ministry of Communications and Technology (MoCT)

The Ministry of Communications and Technology is responsible for developing regulations and frameworks for national policies, legislation, and strategies related to information, communications, and postal sectors. It involves supervising these sectors, setting standards, encouraging investment, and promoting technology's role in economic and social development. Additionally, it focuses on international relations, capacity building, and enhancing administrative procedures through information technology. Furthermore, this ministry leads the efforts in developing national legislation related to communications, international partnerships, and promoting research and development endeavors amongst others (MoCT, 2013).

Syrian Telecommunications Establishment (STE)

The STE is pivotal in the cyber domain in Syria by enabling local Internet providers with global connectivity, effectively regulating the inflow and outflow of information. The STE was established in 1975 and was constituted as a state-owned enterprise in 2012. Although STE is overseen by a Chief Executive Officer (CEO), it operates under significant government supervision. Providing Internet, voice, and data services, it exclusively installs landlines and determines connectivity across regions. By 2010, it served around four million subscribers and formed alliances with foreign companies like Nokia, Thuraya, Samsung, Ericsson, and Huawei. Locally, STE collaborated with Syriatel and MTN, the country's two mobile service providers. The STE exercises control over Syrian autonomous systems, linking the nation to global networks, thus governing inbound and outbound traffic. All international connections are routed through STE, which, along with limited external connection standards in Middle Eastern countries, poses vulnerability to interruptions and communication breakdowns. Tartous

and Aleppo emerge as strategically significant cities for communication control (Racicot, 2015).

The National Agency for Network Services (NANS)

The Ministry of Communications and Technology (MoCT) established the National Agency for Network Services (NANS) in 2009, entrusting it with the mandate to arrange, synchronize, and streamline operations and initiatives across national networks. This entity oversees and regulates various aspects of electronic transactions and network services. Their responsibilities include managing electronic signature services, enhancing electronic service efficiency, monitoring network emergencies, enforcing security measures, and promoting research in network services. Additionally, they control and license electronic signature systems, manage Syrian top-level domains, set security standards for networks and websites, allocate internet addresses, resolve disputes, and offer specialized training in IT-related fields (NANS, 2017).

Syrian Telecommunication Regulatory Authority (SyTRA)

This involves establishing regulations and oversight for the telecommunications sector, covering various aspects like market analysis, licensing, managing resources, ensuring service quality, fostering competition, and representing Syria in global communication forums. It includes defining standards and licensing conditions, ensuring security, and monitoring operators' compliance (SyTRA, 2018).

Syrian Computer Society (SCS)

The Syrian Computer Society (SCS) was founded in 1989 with the aim of promoting and advancing Information Technology (IT) and Computer Science among the Syrian population. Over the years, the SCS has played a pivotal role in the development of IT in Syria, despite being an independent civil organization, it has maintained strong ties with the government. The organization was established by Bassel Assad, the eldest son of Hafez Assad, the former President of Syria, and after his untimely death in 1994, Bashar Assad took over the leadership until his presidency in 2000. The SCS conducts various training sessions, meetings, and conferences to enhance computer literacy and established its own Internet services provider, SCS-NET, which has significantly contributed to expanding IT infrastructure and services throughout the country (Racicot, 2015).

Syriatel

It is the primary mobile service provider in Syria, an exploding market. In 2000, SyriaTel was established with the goal of providing telecommunication services to the

Syrian population. By 2014, it had expanded its network of radio base stations throughout the country and had a customer base of seven million, with only one competitor, MTN. SyriaTel also owns SAWA, one of the largest Internet Service Providers (ISPs) in Syria. However, the company has been facing American sanctions since April 2012, despite which it continued to forge partnerships with Chinese firms. Like other service providers, SyriaTel's traffic is also routed through the STE. The company was initially owned by Rami Makhlouf, a cousin of President Bashar Assad, who also served as its CEO. However, in mid-2020, the Syrian government ordered the confiscation of Makhlouf's assets (Al-Jazeera, 2020).

MTN

It is the only competitor for Syriatel. It was part of MTN GROUP - the South African multinational corporation and mobile telecommunications provider network. MTN Syria provides GSM and 3.5G broadband, including 4G services. In 2020, MTN Group divested 75% of its stake in MTN Syria, selling it to TeleInvest Ltd, a Saudi-owned entity that already held 25% ownership of the company. (MTN Syria, n.d.)

Private internet service providers

In 2005, the first private internet service provider was established. However, the number steadily increased in the following years, and the estimated number of operating ISPs today is 14, including private and state providers. Although this number could give the feeling of competence in the market, however, all connections of these ISPs to the global network should go through STE. Also, ISPs must be subject to the policies and instructions of NANS. Even though some of these ISP owners have deep ties with the government, business leaders intending to launch their services can do so by signing a memo with the STE and getting approvals from the relevant intelligence branches.

4.4. The Role of the Syrian Government in Controlling Cyberspace

The cyber domain in Syria is described as a highly centralized and heavily monitored space. This is already explained by what we mentioned previously about how the cautious Internet entered Syria and the measures taken by STE, limiting access to the Internet to a minimal number of subscribers. This lasted till the beginning of 2005 - as described to be a turning point year- in which the total number of subscribers was estimated to be no more than 30K subscribers. After that, the total number of Internet subscribers increased to approximately 4 million in 2010. But despite this great openness

to the Internet that Syria appeared, which may seem contradictory to the tight security grip and caution that preceded that year, many restrictions were imposed on Internet use. Some have pointed out that the system requires all Internet service providers to monitor all activities that take place on the Internet. Also, with the spread of Internet cafés, everyone who wanted to use the Internet was required to show his identity card upon entry, which the café owner would save a photocopy, record visit duration, and keep a record of his activity at the end of each session (Rey, 2017).

According to documents obtained by Privacy International, STE relied on advanced technology from Western companies that enabled the interception of real-time phone calls, text messages, faxes, emails, and VoIP services. This technology is mentioned to be integrated within various types of infrastructure, whether cellular networks or landlines and from multiple companies. During discussions with providers regarding the desired system, STE emphasized its focus on addressing 'propaganda mail' in the form of spam rather than traditional spam filtering systems. This distinction might imply the development of a system aimed at countering a specific tool of cyber-activism (Privacy International, 2016).

The report, published in 2016 by Privacy International, provided many details on how the Syrian government controlled the cyber domain using multiple technologies, taking advantage of having all internet traffic going through STE servers. The report indicated that STE launched the first nationwide surveillance system in 1999 to monitor mobile and landline telephones and internet communications (Privacy International, 2016). Moreover, in 2007, The STE invited bids from multiple companies to create a centralized internet monitoring system. Further requests were made for a system to monitor and filter content by analysing data packets using keywords or specific patterns. This system would allow for storage, analysis, or even blocking. Additionally, it aimed to track up to fifty targets in real-time, ensuring the monitored users remained utterly unaware of this surveillance. In essence, the Syrian system aimed to have the capability to select and monitor any Syrian individual, track their online activities, and trace their mobile device's location in real-time, all without their knowledge of being monitored.

Moreover, another report by Citizen Lab research centre at the University of Toronto argued that the Syrian regime was using telecommunication monitoring devices developed by Blue Coat Systems; a company based in the United States. This was discovered earlier in 2011, just a couple of months after the outbreak of the protests in Syria. The main objective of these devices is to permit filtering, censorship, and

surveillance over the network. Although the company - which was exposed to be violating U.S. orders as Syria is under U.S. sanctions- confirmed the authenticity logs from Syria but denied making sales to any entity in the country. The company then announced that the devices working in Syria were shipped to a distributor in Dubai to be delivered to another country (Morgan Marquis-Boire et al., 2013). These devices use deep packet inspection "DPI," a sophisticated method used in computer networks to closely examine the content of data packets as they move through a network. It goes beyond just checking packet headers, allowing for detailed analysis of the information transmitted.

Kareem, one of the interviewed cyber experts, worked at Syria Computer Society between 2008 and 2014. Kareem mentioned that SCS has had a direct marine connection to the global network through Cyprus. However, there were many debates by the government about making all connections to the worldwide network through only STE, and Kareem thinks they did it. Also, Blue Coat servers were available in SCS; they were procured through a company in Dubai to overcome the U.S. sanctions.

All interviewed cyber experts who worked within the telecommunications companies Syriatel and MTN confirmed that neither company had any control or decision-making regarding the Internet. Although Kareem mentioned that SCS has had a direct marine link to the global network with Cyprus, he indicated that STE revoked this, limiting access to the worldwide network only through STE. Syriatel, for example, did not have servers that kept logs of the traffic in the network. Omar, who worked in an administrative position at Syriatel in the Damascus headquarters office, pointed out that Syriatel relies entirely on STE to provide Internet. This is because STE is the one that connects to the global network. Also, the Syrian Telecommunication Regulatory Authority (SyTRA) intervenes in the prices of Internet packages, and even if the company wants to present new offers, it must obtain the approval of the SyTRA, which was the main point of contact between the telecommunications company and Syriatel. Regarding Telecommunications, the matter is somewhat different. Fatih, a project manager at the Syriatel, mentioned that any telecommunication company is obligated to keep copies of all calls and mobile messages over the network as in the contracts with STE. It must provide the necessary equipment and access to STE on these servers. Youssef, a network engineer who worked with MTN, pointed out that as an international company, MTN is treated slightly differently from Syriatel. MTN switches and Servers were located in STE buildings. Guards protected these buildings, and no one was allowed to enter without a security clearance. MTN shares a list of names of its staff -whose tasks include dealing

with these servers and switches- with STE. These lists are shared monthly, and the guards, whom Yusuf assumed to be intelligence personnel, check his ID card and ensure that his name is on the list before allowing him in.

4.5. Intelligence Forces Power in Cyberspace in Syria

In Syria, which has been called the "Kingdom of Silence," the authoritarian regime controls all aspects of life through intelligence forces that monitor almost everything. Even the Syrians constantly say that even 'walls have ears' since all that they are speaking or doing is being monitored. The structure of the intelligence apparatus in Syria consists of four central bodies, two divisions, and two directorates. Military Intelligence division and Air Force Intelligence division are affiliated with the Ministry of Defence, while the Political Intelligence Department and the General Intelligence Department are affiliated with the Ministry of Interior. Each of these divisions and departments has a group of central branches that vary according to areas of concern or specializations, and regional branches spread throughout all governorates, whether in cities or villages. Therefore, number of branches is limitless. Each branch is identified by a number and attached to several detention centres. The strength and size of the branch varies according to the region or city in which it operates. These branches assume internal and external responsibilities ranging from monitoring the army forces, police forces and security, borders, and oppositions to monitoring and targeting civil activists (Clinic et al., 2021). In Syria, any activities, especially those involving collective actions such as religious activities, humanitarian actions, and any other collective events, even weddings, are known to have approvals from security authorities.

With a cyber domain that allows people to gather, share, and disseminate information freely, the surveillance state needed specialized intelligence branches to monitor this domain fully. Most of the security branches that we know, whose mission is to monitor and track everything related to communications and information technology, are affiliated with a military intelligence division, which are:

Branch 225 is also known as the Communication Branch. It is the most dominant branch of the cyber domain and all information and communication-related entities. It monitors internal and external communications by phones, mobiles, or faxes. The capability of this branch includes direct control over all communications within Syria, enabling actions like blocking particular numbers, terminating calls, disabling SMS

service for specific numbers, and intercepting or preventing the delivery of messages, alongside the ability to monitor phone calls(Maen Tallaa, 2016). As the revolution erupted in Syria, and due to its cyber roots for coordination, organization, and dissemination of information, this branch turned into complete management. Moreover, officers and personnel were sourced from different branches and departments to support the duties of this branch and have been provided with unique identification cards issued by the presidential palace (VDC, 2013).

Branch 211 Referred to as the "Technical" or "Computer" branch, this division primarily concentrates on internet-related affairs and supervises online operations. Its responsibilities encompass regulating website access, handling wireless communications, and delivering technical assistance to Branch 225. (Maen Tallaa, 2016).

Branch 237 focuses on tracking and tapping wireless calls, specializing in scanning wireless and radio waves (SNHR, n.d.).

Digital security branch is one of several new intelligence branches established by Russia and announced in 2019. This branch is affiliated with the Department of Political Intelligence, specializes in cyber and information security, and is subject to direct supervision by Russian officers (Hiba Mohammed, 2019).

Building on the diversity and specializations of these branches, the Intelligence apparatus has broad monitoring and control over the cyber domain. Their personnel have complete access to surveillance equipment and devices maintained by STE and could have the ability to examine all the activities taking place in the cyber domain (Racicot, 2015).

4.6. International Presence in Syrian Cyber-space

Before discussing the international intervention and responses to the cyber conflict in Syria, it is worth mentioning that the Syrian Telecom Establishment (STE) has been working with telecommunications and technology companies to assist in censorship, implement surveillance systems, and expand monitoring efforts. Privacy International and Reflets.info obtained documents mentioning the names of several ICT solutions companies, some of which are headquartered in Europe and the United States, that impose sanctions on the Syrian regime.

Blue Coat Systems (U.S.A) specializes in Internet monitoring and filtering devices. The Citizen Lab team for Internet monitoring research indicated that the

Telecommix cyber-group, in cooperation with Reflets.info, were able to prove the existence of active devices for this company operating from Syria, which violates U.S. laws in banning the sales of such devices to authoritarian regimes including Syria. Later, when presenting evidence of the operation of its systems on the Syrian network, the company indicated that it had not sold such devices to Syria but rather to a company based in Dubai, acknowledging they were active in Syria, and it had stopped the devices' ability to benefit from its cloud services. However, it claimed that they cannot switch off these devices remotely (Morgan Marquis-Boire et al., 2013).

Advanced German Technology AGT (Germany): This is the most active company in Syria, working with STE and the Syrian government to provide censorship and network surveillance solutions. AGT worked as a "proxy company" or "Broker" for international companies that offer Internet network monitoring and filtering services. This company was registered in Germany but mainly working from Dubai, and later, in 2008, it was registered in Syria under the AGT Syria name. This company was founded by two German-Syrian brothers. It has provided censorship systems to the Syrian government since 2002. AGT actively used it is presence in Dubai to overcome U.S. sanctions and re-route U.S. origin devices to Syria; as one of the company engineers stated to Privacy International: "When I was in Syria, I saw a ton of different USA brands, Cisco, IBM and all of them arrived from Dubai" (Privacy International, 2016).

"In SCS, we used BlueCoat servers for website blocking and filtering. Blue Coat equipment was procured to Syria via a company based in Dubai." Kareem, Software Engineer.

RCS S.p.A (Italy): Milan-based ICT company specializing in communication surveillance and censorship solutions. The solutions include a centralized monitoring system with sophisticated visualization ability and a large-scale subject-related database analysis system. In a partnership with AGT, RCS was implementing one of these solutions (Privacy International, 2016).

VASTech (South Africa): A South African information and communication technology firm specializing in providing surveillance systems to government clients since 1999. VASTech has a tight relationship with AGT. Privacy International revealed that VASTech had provided censorship solutions in Syria since 2002, facilitated by AGT(Privacy International, 2016).

Amesys (France): another partner for AGT is Amesys, a French company. Although the company denied having any contracts with the Syrian government due to

the political situation, it acknowledged providing a surveillance system to the Libyan government in 2007. It admitted that AGT was a distributor of Amesys technologies for the Middle East market. After an investigation by a French court into human rights violations, the company separated it is activities under censorship and surveillance systems and established a new company in Dubai in 2012 (Privacy International, 2016).

Utimaco (Germany): is a cybersecurity and surveillance technology firm from Germany. Utimaco officially provided an interception management system in 2004 to its partner Siemens to be implemented in Syria for approx. 1.2 million euros. This system allows for real-time communication interception and was available until at least 2009. Utimaco stated that this system is no longer available in Syria (Privacy International, 2016). Also, Utimaco was a subcontractor for AREA SpA in implementing the Central Monitoring System in Syria(Champagne - Kitetoa, 2014).

AREA (Italy): another Italian company that provides surveillance infrastructure. AREA won a bid to implement a central monitoring system for STE under the codename Asfador. It then claimed that it suspended work on the Syrian system after It paid a fine to the US Department of Commerce for violating US export regulations. It had a subcontract with the German company Utimaco. According to the reports, the company could not finish implementing the system and withdrew from the country after the breakout of the uprising in 2011 (Privacy International, 2016).

Qosmos (French): Qosmos offered the Syrian STE an intelligence tool called Deep Packet Inspection (DPI). According to Reflet's report on company activities, Qosmos products have been set up in Syria effectively. Qosmos had a subcontract with Utimaco and kept doing business until November 2012. Qosmos claimed they terminated the project in Syria, and its equipment has never been operational (Champagne - Kitetoa, 2014).

On the other hand, all interviewees working in Syriatel confirmed that by 2009, Syriatel had replaced all its infrastructure with Huawei, the Chinese manufacturer. They rebuilt the core network and installed many modules. “Huawei helped with telecommunication censorship as they were very effective in this field. Regarding Internet censorship, I am sure that the monitoring was not from the Syriatel's side, but from the STE's side,” Ziyad said. Omar confirmed, “I have met some experts from Huawei corporation that provided infrastructure, but they were only providing some minor technical support, and currently, they are unavailable.”

4.7. Cyberspace as a Tool of Repression

As we already discussed, it can be argued that the Syrian regime has a solid surveillance infrastructure that started building once the internet was allowed to enter the country and started with making the STE the only establishment connected to the global network, as well as obligating all other ISPs and telecommunication companies to comply with the regulations and policies imposed by the STE. Moreover, various intelligence branches monitor communications and track online activities. On the other hand, insufficient expertise in secure communication, encryption methods, and digital safeguards led to breach the privacy rights among cyber-activists. It made them vulnerable to personality identification, tracking, and targeting (Al-Saqaf, 2016).

Privacy International argued that cyberspace in Syria is used as a tool for surveillance and censorship by employing various monitoring strategies. These strategies include restricting global connectivity to the Internet to STE and routing the whole country's Internet traffic through its servers. Moreover, STE worked as a front for the intelligence apparatus, namely branch 225, which is known as the communication branch. A Syrian computer specialist reported to PI that recalls that any communication service providers coming from outside the country will have security officers attached to them wherever they go. Moreover, ISPs in Syria requested to keep logs of internet traffic for six months, and the branch 225 personnel could come any time to request a copy of the entire log. (Privacy International, 2016). Amjad Baiazy, a Syrian cyber-activist, stated that STE has a central operations room with surveillance system which is directly linked to Branch 225 Damascus (Baiazy, n.d.).

A study by the Syrian Center of Media and Freedom of Expression showed that between 1999 and 2005, the general policy of Internet Server providers, which were only STE and SCS, was “Block everything and allow some services.” As mentioned earlier, many services like email and FTP were blocked. After 2005, the policy was changed to “Allow everything but block some services”. According to this study, blocking was two types: services and websites, and both are under STE control by request from intelligence branches. The type of blocked websites is not limited to harmful content; instead, it seems to be focused on two main objectives:

- Preventing Syrians from publishing content on the Internet, such as blogging websites and other online journals from Syria.

- Preventing Syrians from accessing content that is not desirable to decision-makers, such as blocking many websites in Arabic content and several safe browsing services that allow bypassing the blockage (Scmadmin,2011).

In 2012, approximately a year after the protests in Syria, the President introduced the "Informatics Crime Law," or Cybercrime law which aimed to govern online communication and cyber-related crimes. This law, subject to multiple amendments—most recently in 2022—transforms the cyber domain, potentially subjecting users to legal consequences for expressing opinions. It mandates website owners to archive their content and traffic data to verify contributors' identities, necessitating the disclosure of their identities and content to the government. This provision facilitates the tracking of Syrians through their online presence and holds service providers responsible for maintaining contributor information, even over extended periods. Furthermore, the law criminalizes the dissemination of false news that could damage the state's prestige or national unity, thereby placing civilian activists or journalists at risk of arrest (Tounsi & Zouai, 2022).

Many research centres, such as Citizen Lab, published reports on digital surveillance in Syria and how the Syrian regime uses cyber capabilities to trace activists, which leads to arrest, torture, or even killing of the dissents. A researcher called Fredric Jacobs, who was working with an international company contracted with STE, stated that every bit of data flowing through the Syrian network is meticulously stored on hard disk drives controlled by the Syrian regime, including vast amounts of information (Clinic et al., 2021).

4.8. Incidents That Illustrate the Government's Control over Online Activities

Despite allowing publishing in a seemingly free manner as of the beginning of 2005, and despite the lack of prior censorship on what is published, Syria has witnessed several cases of arrest or trial because of online posting. Muhammad Ghanem, founder and director of the Souryoun website, was arrested on 31 March 2006 due to media materials published on his website. Mohammad was sentenced to six months in prison by a military court on charges of insulting the head of state, inciting sectarian strife, and undermining the prestige of the state (Scmadmin,2011).

In 2009, Tal Al-Mallouhi, a 19-year Syrian blogger, was considered "the youngest Internet Prisoner" in the world. She was taken from her home by intelligence forces. A

public statement by Amnesty International explained that Tal was arrested on 27 December 2009 by the State Security branch, most probably due to her activism on the internet. Tal is an active blogger, and “she has published poems and articles that she has written on various political and social issues” (Amnesty International, 2011). Before detention, Tal was repeatedly called in for questioning by the general security branch because of her online posts and blogs. During one instance, she was asked about the Syrians she was contacting online who were living abroad, and she was cautioned against sharing any information online by contacting newspapers. In February 2011, Tal was sentenced to five years, and this incident was one of the most prominent cyber-activist detention cases, which led to an increment of Syrian people tension. One month later, many protestors in the streets of Homs City were calling for “Freedom for Tal Al-mallu,” but she is still in detention.

Another case about detention due to online activism in Syria was reported in a study titled “DIGITAL DOMINION: How the Syrian Regime’s Mass Digital Surveillance Violates Human Rights” by John Marshall Law School International Human Rights Clinic. Akram Raslan, a cartoonist, works at a local newspaper and contributes to multiple news websites at his workplace. It was later claimed that he was arrested over cartoons deemed to have "offended the state’s prestige." Akram completely disappeared after his detention, and subsequently, in 2015, it was reported that he suffered torture to death in 2013. (Clinic et al., 2021)

Ziad mentioned in Syriatel, “Through the Mobile Switch Centre (MSC), we could detect the location even for switched-off devices. We also can get information on a specific call from where it was made.” Ziyad explained. He mentioned that the requests to track the location were coming mainly from the intelligence branch 225 and, in some cases, from STE. In late 2011, a list of more than 10,000 contact numbers was leaked from Syriatel, containing the numbers to be tracked, and all the calls are being eavesdropped on. “The president's cousin asked to track his girlfriend and know where she was going. He did not want the Telecommunications branch to know about his request, so he requested through STE. Can you imagine this dirt?” Ziad said while laughing.

4.9. Surveillance System and Censorship

After the outbreak of protests in Syria, Omar mentioned that Syriatel implemented special filters on Short Message/Messaging Service (SMS). “Any SMS containing location, time, and date information will not be delivered; you will see an error after sending that the message could not be delivered,” Omar explained. This was a way to hinder the call for demonstrations and share information about the locations of protests. Moreover, Ziyad said that STE requested that some added value services, such as SMS broadcasting, be blocked through any unauthorized company. Only companies registered with STE can use this service. This is because rebels succeeded in using servers outside Syria to send anonymous messages to many mobile subscribers, encouraging them to demonstrate against the Syrian regime.

4.9.1. Censorship: blocking websites and services

Syria developed a custom model of censorship that included blocking unwanted websites, allowing anything to be published from inside Syria, and then holding accountable those who publish unwanted material. Between 1999 and 2005, Syrian Internet users were deprived of most Internet services, as every website containing the word Mail in its name was blocked to hinder the use of email. (Scmadmin,2011)

Since the beginning of the Internet in Syria, many services that are usually available with the availability of the Internet have been blocked, such as the (FTP) file transfer service, which has hindered the publication of Syrian websites on the Internet. Publishing websites require the FTP service, and Syrian websites were limited to a few numbers (Scmadmin,2011).

This included most of the popular services that enable access to email via a browser, such as Hotmail and Yahoo. Mail and others, and many websites that talk about email technologies, such as www.sendmail.org. At the same time, services for sending and receiving e-mail directly via Internet servers outside Syria were blocked. This blocking made sending and receiving e-mail impossible in Syria and contributed to delaying Syrian society’s use of the most straightforward techniques for exchanging information over the Internet (Scmadmin,2011).

This blocking policy continued to be in effect until mid-2005, when the blocking policy was changed to "allow everything, block some services." The same policy was applied to all Internet service providers (Scmadmin,2011). Blogger, Facebook, YouTube,

and Twitter were blocked until February 2011, just one month before the outbreak of the revolution.

"Everything you do over the network is recorded: calls, SMS, MMS, or anything," Fatih said. He pointed out two ways to request this recorded data: the STE has direct access to all servers, but sometimes they [Intelligence] directly request Syriatel to provide records and full communication recording for a specific person in a particular period. Ziyad added that after May 2011, the Intelligence Telecommunication branch was given access to all Syriatel servers.

All interviewees mentioned that telecom companies cannot monitor internet data traffic. "Technically speaking, this is done by STE because Syriatel was only a service provider and not connected to the global network. We did not have such systems in Syriatel," as Ziyad said.

In the Syrian Computer Society service provider, Kareem pointed out that they used Blue Coat servers for website blocking and filtering. As mentioned, Blue Coat equipment was procured to Syria via a company based in Dubai, probably AGT.

4.9.2. Location tracking

One of the capabilities that the Syrian regime utilized is the ability to track the location of any SIM card on the network. Youssef said, "In terms of using location tracking before the crisis, we could track the live location of any SIM card. There was a case where some stations located outside cities, mainly in open rural areas, were equipped with air conditioners to cool the internal devices of the station. These air conditioners were being stolen repeatedly, and the cameras could not track their location because they were in geographically remote areas. To overcome this, we placed a mobile phone inside the air conditioner, and when the device was stolen, we would track its location, find out the thief's whereabouts, and then inform the police about his location. This case, for sure, was in direct coordination with the security and police and technically through MTN.

In summary, the Syrian regime has extensively utilized the cyber domain as a tool for surveillance and censorship by employing various strategies to monitor cyber-activities and track users, especially cyber-activists, through establishing sophisticated surveillance systems, prosecuting people who express dissenting opinions or sharing critical content to regime imposing strict censorship on content and services, enacting laws and regulations that grant authorities extensive powers to control online activities and finally creating an atmosphere of fear and self-censorship, by physically targeting cyber-activists and subjecting them to arrest and even prosecution.

4.10. The Impact on Freedom of Speech and Human Rights in Syria.

Freedom House, an organization based in Washington, considered the cyber domain in Syria to be an "acutely dangerous environment to journalists and online activists" due to challenges in accessing, restrictions on content, and user rights violations (Freedom House, 2020). Moreover, Syria was mentioned amongst countries highlighted as "enemies of the Internet" by Reporters without Borders (RSF) in 2014, owing to its repressive measures that severely curtailed freedom of expression online (RSF, 2014).

Apart from the detention and arrest by intelligence forces, a Digital Dominions study stated that Syrian authorities appointed 58 judges to supervise prosecution trials related to "Informatics Crime law," also known as "Cyber-Crime law." These judges -whose independence is questionable- are reported to be trained in social media, web content filtering, data collection, and information systems. It also mentioned that surveillance systems have facilitated censorship of the internet, which exposure cyber-activists to arrest, torture, and execution due to online civil activism (Clinic et al., 2021).

On the other hand, after the outbreak of protests in Syria in 2011, which relied mainly on the Internet, it was described as "the most documented crisis in history" due to the large number of videos, pictures, and news that spread on social media and the events which were documented daily by cyber activists. As a result, the number of arrests, tortures, or deaths of cyber-activists increased dramatically. Many online activists reported being arrested, threatened, tortured, or have gone missing due to their online activities and the use of the internet. American journalist Marie Colvin – who worked as a foreign affairs correspondent for British the Sunday Times and entered Syria secretly in 2011- was reported to be pointing her location by scanning her satellite phone transmissions with the support of Iranian software. (Margaret Weiss, 2012).

The Digital Dominions study referred to an interview with a Damascus University student who was subjected to investigation by the Student Union -which became known as a supportive body to the army and security forces in suppressing protests in Syria after 2011- the student indicated that the student Union was monitoring his social media accounts. He was summoned to the Student Union office. The officers in Student Union presented to him a screenshot of a Facebook account of one of his friends, which contained undesired posts. Although he was not arrested, he has become more cautious and has tightened his self-monitoring of what he posts online and overall cyber activities (Clinic et al., 2021).

On a final point, The Syrian regime has implemented extensive surveillance and censorship measures to control the cyber domain. Starting with the STE as the sole gateway to the global network and as a front for intelligence forces, monitoring communications and requiring ISPs to retain internet traffic logs. Furthermore, STE employed Western technology for real-time surveillance of communications. Reports indicate STE's nationwide surveillance system since 1999 and its bid for advanced monitoring systems by 2007. Blue Coat Systems' devices for filtering and surveillance were reportedly used in Syria, violating U.S. sanctions. Syriatel and MTN, major telecom companies, had limited control over internet and telecommunication services, with STE overseeing and regulating most activities. Consequently, policies shifted over time, initially blocking most internet services and later focusing on content control. From 1999 to 2005, most internet services were blocked, including FTP and popular email services. Then the policies shifted again in 2005 to "allow everything, block some services," but platforms like Blogger, Facebook, YouTube, and Twitter were blocked until 2011. On the other hand, the 2012 "Informatics Crime Law" tightened control, requiring website owners to archive content and verify contributors' identities, while criminalizing the dissemination of what they called "false news." Subsequently, the extensive documentation of the 2011 protests led to increased arrests and abuses of cyber-activists, and the emergence of cyberconflict.

CHAPTER V

5. THE RISE OF CYBERCONFLICT IN SYRIA

5.1. Cyber Activism in Surveillance Zones

With the outbreak of protests in Syria in mid-March 2011, cyberspace became the safest domain – as considered by activists as all gathering places were under monitoring. Therefore, cyberspace has become a place for organizing, sharing ideas, mobilizing, and coordinating activities. Thus, the cyber domain became the major battleground between the Syrian regime and the protesters. Social media played a significant role in the spread of demonstrations and the dissemination the picture of brutal repression against protestors across the country, with a complete absence of independent news channels or international press. In a study titled "Syria's cyberwar," Amjad Baiazy – a Syrian activist-met a cyber-activist activist from a town in Daraa city who explained the role of cyberspace in activism in Syria, "I never used the internet before the revolt, but as the revolt started, I felt obliged to tell the world what was going on in my town. So, in a few weeks, I became a reporter for many TV channels. I used Skype and satellite phones to communicate with TV and social media to spread news worldwide. Then I started training others, and now we are a group of twenty-five media activists in my town" (Baiazy, n.d.).

5.2. Cyber Domain: A Mobilizing and Coordination Space

Social media networks, including Facebook, YouTube, Twitter, and blogging websites, have been blocked since 2007 as an STE and intelligence apparatus censorship procedure. Surprisingly, the Syrian regime removed the blockage on Facebook and YouTube in February 2011. It took this action just weeks after the successful use of social media in Egypt to mobilize thousands of anti-government protests and a few weeks before protests in Syria. On one side, unblocking Facebook could allow the activists to share information and utilize it for coordination and mobilization, but on the other side, this meant they would now abandon any safety software were used to access the website, and this could put the activists under risk of being detected by the government as Baiazy explained (Baiazy, n.d.). As a result of unblocking Facebook, for example, Racicot stated that "From January 2011 to April 2011, the number of Syrian Facebook accounts increased by 192,732, reaching a total of 356,247 by May 2011." (Racicot, 2015, p.23).

“Since screening operations of Internet traffic had been in place for years, enabling Facebook and other social media allowed the government to quickly locate those opposed to the regime and map the social networks of protesters to locate local leaders” (Racicot, 2015, p.24).

Ahmad, a cyber-activist from Homs who has been involved in many activities related to the cyberspace conflict, stated, “I created my first account on Twitter in 2009, but I never knew how to use it. I created it using my real name. I never understood how it worked and was ineffective at it. Also, I created an account on Facebook, which was blocked then. I used a VPN application to access the website. Moreover, I created a blog on WordPress. The topics I was writing about were just diaries, a book summary, and some articles on social life matters. For me, it was just a new space. But things changed completely after 2011, with the beginning of the revolution.”

Ahmad continues: “The beginning was terrifying for me because of my weak knowledge of how to protect myself over the Internet. I was posting on Facebook about the events taking place in my nationhood because police checkpoints separated the regions in my city to hinder the protests. People could not know what was happening in nearby regions without sharing the updates on Facebook. Then, I started to write more to encourage people to demonstrate against the regime. After that, I started organizing demonstrations under “coordination units,” groups on social media to share ideas and organize protests. In these coordination units, each member has a task; for example, someone knows how to create designs using Photoshop, another knows how to write posts, another knows photography and video editing tools and other works on publishing and sharing on the Internet. We were using social media under fake names; in each group, we did not know each other for security reasons because if one of us who knew the names was arrested, this would put all of us at risk. Trust came in a network form: I know and trust X, and X knows Y and Z, I will coordinate and trust Z without in-person knowing.”

Abdulkadir, an activist in the capital, Damascus, said, “We used Facebook mainly with fake names; we used to coordinate with people sharing the same objective without knowing their names. We trusted each other in a network way until we reached a group of 150 people coordinating the protests in Damascus.

Regarding selecting tools and platforms for activism in cyberspace, Ahmad explained, “I was much more active on Facebook than Twitter because most Syrian people were on Facebook, while Twitter was not active. I remember in 2011, I had about a thousand followers on Twitter, then the number doubled in the following years. After

2014, I switched to Twitter to share information with audiences outside Syria, especially in the Arab world. I was not active on the blog because the activism was quick writing, situation updates, and breaking news, as people did not follow long articles."

Samer, a computer engineer and cyber-activist living abroad when the protests in Syria broke out, mentioned, "I was not active on Facebook or any other social media platform. I was not good at posting and interacting with others, but I wanted to participate. With the support of friends, we developed an interactive map that shows the locations of the demonstrations with a bubble presenting the estimated number of protestors. This aimed to show the spread of protests a regime, which can encourage all areas to participate. Although the impact of this map was limited because agencies are more interested in photos and live videos, it was a nucleus for forming a cyber-activist group that started live video streaming to fill the gap of the absence of news agencies and media networks.

Samer explained, "We were a team of no more than 15 people inside and outside the country. The broadcast solution was as follows: a computer, a converter card, a camera, and a software application connected to a server in Canada. We worked with Al Jazeera, Al Arabiya, Sky News, and CNN. Al Jazeera was the channel we worked with mostly. This live broadcasting of protests was essential to make people feel that the revolution was spreading, the regime was losing control, and no one was afraid anymore. We also focused on mobilizing people in the capital, Damascus. We succeeded in broadcasting directly from the Damascus neighbourhood, Kafr-sosah, an area full of intelligence branches. We thought that this would break the regime's propaganda. We also broadcasted from the besieged city of Homs to encourage people to continue their activism and raise their morale."

5.3. Authoritarian Countermeasures: Intelligence Forces Response

Matthew Rey, in his study on how the Syrian regime tried to prevent mobilization spreading, said that cyberspace in Syria was a helpful tool for intelligence forces to track activists. Consequently, activist groups coordinating on Facebook, such as local coordination units, were tracked and exposed to arrest. During their arrest, intelligence forces used physical torture to get their social media credentials and deploy malware that permitted them to spy on computers leading to heightened distrust. Consequently, an expert cyber-activist group called "Anonymous" assisted activists by implementing

advanced secure browsing tools like Tor, and trained activists on using VPN (Virtual Private Network) to be more protected (Rey, 2017). Moreover, cyber-activists who established direct communication with Facebook contacted the company to close the account for activists immediately after they learned of the arrest incident.

Racicot mentioned that Syrian authorities were slowing down internet transmission speeds on Fridays, known as the day of the demonstration. This technique is used to hinder any use of the cyber domain in uploading videos and photos or using the internet for live streaming, and this also will allow for real-time traffic monitoring. Moreover, a complete shutdown of the internet was reported from different regions in Syria concurrently with massive protests or military operations. For example, all Internet connectivity was turned off in conjunction with massive demonstrations in Hama, including the entire mobile data network, to obstruct the mobilization and dissemination of information (Racicot, 2015).

On the other hand, (Clinic et al., 2021) mentioned that branch 225 ordered mobile operators in Syria, namely MTN and Syriatel, to filter and block any SMS containing words that indicate coordination or participation in a protest.

“We used text messages to indicate participation in a specific demonstration, for example, ‘The lecture today at the university is at noon’ which means that the demonstration will be afternoon prayer. After several weeks, we noticed that any message indicating a time or location would fail to be sent over the network.” Ahmad stated.

5.4. Overcoming the Digital Curtain: Navigating Internet Blackouts

Cyber-activists overcame internet blackouts and transmission bandwidth restrictions by using connections beyond STE, such as satellite internet and internet connections in nearby countries. Satellite Internet devices were smuggled through borders and used by activists and journalists to share updates and broadcast events. After a time, satellite services were available for everyone with subscription packs, especially in out-of-government control areas. On the other hand, accessing the Internet from nearby countries was a cheaper alternative. Still, this option was limited to regions close to international borders, such as Daraa in the south with Jordan and northern border regions with Turkiye. Jordanian mobile sim cards and network coverage were affordable in Daraa while laying down cables and wireless connections across the border with Turkiye were accessible in the northern region. These solutions helped access the Internet at high

transmission speeds and provided a safe environment by bypassing all censorship mechanisms that STE had placed on the Internet. Also, it became the only means of connecting to the Internet after the regime cut off communications over out-of-control areas (De Angelis & Badran, 2016).

Abdulkadir stated, “Accessing the Internet was a big challenge. I remember that in the first or second week of the revolution, two demonstrations took place in Damascus, and the regime cut off the Internet in all of Syria. One of the young activists recorded the demonstration, loaded the files on a flash drive, and repeatedly transferred the flash drive from one person to another until it finally reached Daraa in the south of Syria to be uploaded to the Internet using a Jordanian sim card. That time, we started searching for alternative solutions.”

Regarding protests live video streaming, Samer pointed out, “We initially attempted to use the existing internet in Syria around 2011. We tried using internet networks using a SIM card registered with the name of someone outside the country to avoid putting anyone at risk of arrest. However, the picture quality was inferior due to the regime's practice of reducing or cutting off the internet in areas with live streaming. We had a compounded fear—no one dared to use a SIM card registered under their name in case it was deactivated. Therefore, it was not a sustainable solution, especially since the regime could cut off the internet at any moment.” Consequently, Samer searched for solutions for internet connections; he said, “We started using satellite Internet from Al-Thuraya company based in the United Arab Emirates, then we switched to Inmarsat, which is European, due to security and protection reasons. We provided activists with satellite Internet to broadcast live video and replace local internet use.”

5.5. Intervention of the Intelligence Branches

In Syria, the intelligence branches have comprehensive monitoring capabilities in the cyber domain, with access to surveillance equipment maintained by STE. This enables them to monitor and control online activities effectively. Moreover, they were extensively monitoring all activities inside telecommunication companies.

Omar said, "It is forbidden to have any political debate inside Syriatel.” We can assume that this was a standard coping mechanism by employees as the cousin of the regime president owns the company. During the early days of the crisis, Syriatel started disconnecting SIM cards; for example, all the SIM cards linked to stations in the

geographical areas opposing the regime. However, the leak of a file containing all the SIM cards required disconnecting them. This leak led to a significant investigation; many employees were investigated, and some were arrested. Ziyad pointed out, "As of May 2011, Syriatel was transformed into an intelligence branch, where a security detachment was placed inside the company. Also, the guards at the main gate changed to intelligence personnel, and there was a colonel who was completely responsible for security matters moving inside Syriatel offices with a military uniform and Syriatel ID". Ziyad added that "many employees were arrested due to leaking information. Yamen, one of his friends, never joined any protests or had any activity outside the company, but rather, he was arrested due to information leaking and was martyred under torture. Some of the detainees are missing till today".

On the other hand, Yusuf in MTN pointed out: "During my work, I did not realize the presence of intelligence personnel within the company." This intersects with Ziad's explanation that the regime treated MTN as an international company, which differs from Syriatel.

In SCS, Kareem mentioned that in the early days of protests, we received multiple requests from Telecommunication Branch 215 to get information about specific IPs, for example, the telephone number used to access the internet. Also, they were requesting a copy of traffic to particular users. By 2012, the telecommunication branch had access to all traffic by installing mirroring servers in one of its buildings in the Al-Muhajreen neighbourhood in Damascus.

5.6. Defying Digital Oppression: Cyber Protection Tactics

The awareness among activists of potential regime monitoring in cyberspace prompted them to take preventive measures, yet the full scope of the regime's surveillance capabilities exceeded their expectations. Consequently, they adopted diverse methods to conceal their identities and activities. Ahmad said, "My initial action was changing my name on social media to a pseudo name. This decision stemmed from two primary motives. Firstly, it aimed to grant me the freedom to express myself without being judged based on my identity, ensuring that my thoughts were not directly associated with my name. Secondly, it was a precautionary measure to conceal my identity from potential surveillance, evolving into a pure security concern over time.

On the other hand, Ahmad sought advice from friends to surf the internet securely: “A tech-savvy friend advised me to employ protective software like Tor or VPN to safeguard my identity when logging in. Also, I made it a habit to log out after each session, and caution became the cornerstone of my online behaviour. Yet, amid this vigilance, an inherent curiosity drove me to explore an unfamiliar digital landscape and discover previously unknown information. Many individuals within my network operated under pseudonyms, fostering a trust network where mutual connections made introductions. We joined groups of unfamiliar persons, relying on indirect acquaintanceships for trust verification.

Abdulkadir pointed out another preventive measure: obtaining Internet subscriptions with names that the regime cannot arrest so they can work more freely on the Internet. He said, “We started by dealing with hotel managers cooperating with the rebels. They provided us with photocopies of Passports for Iranian visitors mainly. We purchased SIM cards from cooperative mobile phone retailers to have somewhat secure access to the Internet and communication. Because we have doubts and do not know the regime's telecommunication and Internet capabilities.”

Over time, specialized resources emerged, offering insights into security measures, pre-empting hacking attempts, and immediate response protocols following a breach. Continuous updates were disseminated based on evolving experiences. Additionally, guidance from websites catering to cyber activists focuses on methods to counter government surveillance, bolster security, and select appropriate software for enhanced privacy.

Wafi, as a computer engineer, was supporting other friends in securing their presence over the network. He explained, "My educational background in computer engineering taught me to use specific programs such as VPNs to bypass ISP and access the internet from internet cafes. As for Skype, I strongly believed that it was secure and could not be monitored, but now I have some doubts. Our knowledge of safeguarding ourselves from hacking and espionage relied on shared information and collective awareness rather than formal training among other technically inclined individuals. Even during my studies at the university, we exchanged ideas about these protective programs. Our approach to the cyber domain seemed somewhat naive. We lacked comprehensive knowledge, even among technically oriented individuals, on how censorship could occur. However, our learning stemmed from various experiences and stories we encountered.”

The proliferation of social media has presented challenges for regimes attempting to control and identify activists, leading to a shift in tactics. Instances of arbitrary arrests at military checkpoints have surged, with soldiers requesting individuals to open their Facebook accounts as a means of verifying non-activist status. However, this approach revealed the necessity for these officials to possess social media literacy and internet proficiency. “I vividly recall a checkpoint incident where I was asked to provide my Facebook account to the officer, and I humorously claimed to have forgotten it at home. This highlighted unawareness of cyber matters within the regime personnel, compounded by the lack of surveillance technology. With the expansion of Iran's presence in Syria, security officers appeared to be training on social media, enhancing their awareness and building their cyber capacity.” Wafi stated.

Abdulkadir also highlighted this lack of capacity in tracking and monitoring: “We received information from friends working in internet service providers that the regime had access to logs and keeping a record of anyone accessing Facebook and monitoring activities. From that day, we were cautious; we started indirectly using translation websites to access Facebook or VPNs. We also knew mobile phones and communications, especially SMS, were censored. We did not have a clear idea of the extent of surveillance, but for us, it meant potential arrest at any moment. Also, we knew from friends with advanced technical skills that the regime could not track everything, especially with widespread protests and field-level activism. They focused on key figures and community leaders to track and analyse their movements. In some places, for example, they put surveillance cameras to see who is involved in protests, but they lack technical personnel to extract the data from desks to analyse. Consequently, they returned to the old-fashioned way by arresting one participant and beating him to reveal the names of other participants.”

Cyber-activists used then to have two accounts on social media, a clean one to present to checkpoints and another one used in cyber-activism: “I maintained two Facebook accounts: one bearing my real name and details, devoid of any political narrative. This was a strategic move, ensuring I could access this account without compromising sensitive information if I were ever detained or asked to present my social media account at a checkpoint. Despite adopting advice and insights from experienced friends, the unique circumstances in Syria left me uncertain about the extent of surveillance by the regime. Nevertheless, I retained a basic confidence in my actions and decisions.” Ahmad explained. Similarly, Abdulkadir mentioned: “We changed our

names on social media with fake ones to protect identity recognition. At any moment, a request from the checkpoint to access your online account could occur. Hence, almost every cyber activist had both real and fake accounts."

5.7. Digital Detention: Arrests Stemming from Cyber-Activism

Even with extensive precautions to safeguard their identities, cyber-activists found themselves vulnerable to arrests by intelligence services. Abdulkadir claimed that "Some of my friends were arrested for a like on Facebook page, and others were tortured for liking pages of Al-Jazeera or the Syrian Revolution page on Facebook."

Due to his son's cyber-activism, Wafi's father was summoned to investigate one intelligence branch. Wafi explained, "The first live video streaming I did from the city of Homs using ADSL internet connection. I climbed to the roof of my house, opened my laptop, used my laptop camera, and through a Skype video call, we streamed the first demonstration live on the Al Jazeera channel. The subscription was under my father's name. Just one week later, my father was summoned to the intelligence branch in our neighbourhood. After that, I immediately left the country. We were unsure if it was because of this incident, but mostly because none of us had any other activities."

Ahmad was arrested four times, one of which was because his mobile phone was searched at a checkpoint; the officer found a video of him at one of the demonstrations. "There was a video on my phone of a demonstration, and when the checkpoint searched my phone, they arrested me immediately" Ahmad said. During the detention, Ahmad was asked to provide his accounts on social media, "During one arrest at Branch 215, the investigator asked for my social media accounts; I offered him a Skype ID, and then he said: no need for the password because we can hack it! Specifically, at Branch 215, they asked about my activities on Skype and Facebook.

The investigators were using the detainees' social media accounts, communicating with their friends list, trying to track them down, find out their personalities, and arrest them. "A person in my neighbourhood was arrested, and while he was in custody, someone opened his Facebook account and chatted with his friends, entrapping them. Within 24 hours, we contacted an expert who connected with Facebook, and we closed the account. After that, it became a routine that whenever someone was arrested, we would reach out to people abroad who had connections with Facebook to close their accounts." Wafi said. Likewise, Abdulkadir mentioned," In one case, the

intelligence personnel used a Skype account for an arrested person and communicated with friends' lists. They succeeded in entrapping one of his friends and arrested him. Following this, we began to use signs or a kind of handshaking before we started conversations over Skype."

In Wafi's opinion and experience, "It seems they [intelligence service] were targeting tech-savvy individuals. My name ended up on the wanted list at Branch 225, the telecommunications branch, because I provided satellite internet to activists in Syria."

5.8. Overcoming Censorship: Satellite Internet as a Tool against Restrictions

As mentioned earlier, cyber-activists initiated a search for alternatives to the local internet due to growing awareness of surveillance, the regime's periodical shutting down of the internet during protests, and the complete shutdown of internet and telecommunication from areas outside regime control. Samer contacted retailers selling Thuraya satellite solutions for telecommunication and the internet. However, over time, it was noted that some activists using these devices were subjected to arrest. Also, after his release from detention, one of the well-known activists in Syria indicated that all the calls he made using these Thuraya devices had their details written and printed and were presented by the investigator as evidence of his activity against the regime.

Samer said: "Upon learning about the reported security collaboration between UAE and the Syrian regime and getting information from multiple sources that calls seemed to be monitored, it raised our concerns. I know someone who used Thuraya and has hidden the device in the bathroom. The intelligence forces raided his home, arrested him, and tortured him to give them Thuraya device. He then confessed, and the device surrendered. This incident shattered our trust in the company. Consequently, we shifted to Inmarsat, a European-based company. However, their satellite and internet services were costly. Also, we dealt with companies like Astra and tooWay. Transporting these devices was cumbersome for smugglers. We used satellite internet aiming to evade surveillance, as we believed that whenever the regime allowed internet coverage, it was to monitor traffic over the network. We thought the regime could locate these devices, but we perceived this as a complex task and believed it could not precisely pinpoint their locations. Some of these devices were even in areas subjected to bombings, yet none of these devices were targeted in the attacks."

Similarly, Wafi stated, “One notable incident involved Thuraya, a UAE-based company, where multiple occurrences revealed speaker device coordinates, leading to targeted assassinations based on their location. These incidents often hinted at collusion between the UAE and the regimes.”

5.9. Empowering Cyber-Activists Through Training and Support

It seems the training and support of cyber-activist groups was limited. No reports mention the international support that hacktivist groups received in terms of training or providing programs that help in hacking. Barrow explains that civilian journalists were trained to safely avoid Internet censorship and surf and send media materials (Barrow, 2022). Also, most cyber-attacks by multinational teams such as Anonymous were voluntary and unorganized and were not supported by any country, organization, or governmental entity. Moreover, cyber activists paid for satellite Internet subscriptions, for example, or relied on friends abroad to donate to pay the bills for these subscriptions. This constituted a substantial financial burden on these cyber groups.

Samer, who was working on finding solutions for live video streaming and alternative internet access devices, said: "We did not receive any training or support from anyone. Other media teams received training in Turkey for individuals outside Syrian territories funded by American and European sources."

5.10. The Transformation and the Demise of Cyber-Activism in Syria

In the early days of the Syrian revolution, using social media in discussions, sharing ideas, and self-expression directly impacted mobilization and encouraged people to join the cause. “I believed that abandoning cyberspace would create a void in our activism. However, after the first year, the dynamics shifted, and real-world presence became paramount, overshadowing cyber presence and activities. This shift occurred due to the increasing arrests, martyrdom, and displacements, coupled with military dominance over the political landscape and a lack of international response despite extensive coverage.

Ahmad continued, “The impact of rallying on social media decreased while witnessing daily killings, destruction, displacement, and global silence further diminished its influence. Some friends left the country, while others were detained or became

martyrs. The situation evolved into pure militarism. This shift affected the interest in Cyber Space activity, weakening its impact. Now I am checking one of my Facebook pages; it has hundreds of thousands of followers; however, the last post was in 2016."

From all interviewed cyber-activists' perspectives, civil activism gradually shifted towards militarization post-2012. Simultaneously, many cyber activists diverted towards humanitarian work, prioritizing providing food and shelter for the increased numbers of displaced people. Additionally, the interference of various entities for private purposes, political rivalries, partisanship, and the drift towards militarization collectively diverted attention from cyber-activism. "I see that cyber activists started to leave cyberspace due to severe violence and brutal repression exercised by the regime, coupled with a silence of the international community and lack of response," Wafi said.

Moreover, the lack of support, primarily individual-based, made cyber-activism, such as live broadcasting, extremely costly. Samer explained the reasons behind the conclusion of their initiative: "Personally, costing us over $200,000. The cost per minute was $4 to $5. We attempted to secure support for our content to channels like Al Jazeera, but they declined to offer financial assistance. Additionally, Al Jazeera recruited some of our team members, which weakened our group. Our activism was not institutionalized; it relied on the individuals' enthusiasm. The absence of a person had a detrimental effect on our work, as we could not find someone to fill their role."

On the other hand, the expansion of arrests, the infiltration of some groups that coordinate demonstrations, the absence of detainees, and the brutal torture of them, along with the decline of their influence on reality, led to the deterioration of cyber activity. "In 2013, we started losing momentum of cyber-activism as we noticed an infiltration of coordination groups, which affected our trust. It seems someone has been leaking information about the protest's locations to the regime. In one protest, security forces stormed within minutes and arrested many women. In another one, 15 of our friends were detained. Concurrently, some areas were slipping out of the regime's control, and it was possible to coordinate physically in free zones without risking detention. Also, we believe that our message has reached the world. Our virtual groups shifted from coordination to news dissemination and documentation of events." Abdulkadir stated.

Cyber activism greatly facilitated people getting to know each other, building networks, and establishing communication and organization. Most of these virtual networks have turned into close personal relationships. Despite significant ideological differences, these variances did not harm the work due to the mutual trust and objective.

Samer said, “What brought us together was solely this work. It was based on trust and goodwill, with our goal to support the protests and political change.”

Ahmad said, “All the virtual groups and networks transformed into friendships, professional connections, and other relationships. Many acquaintances I met after leaving Syria were my virtual friends, whom I knew by fake names.”

Similarly, Abdulkadir pointed out, “The groups evolved into forums for exchanging ideas on breaking the siege and sharing experiences. For instance, discussions would include smuggling someone the regime wants out of the country. These groups later transformed into personal relationships. The most notable aspect was the trust placed in pseudonyms.”

In conclusion, Despite facing formidable challenges and countermeasures from the authoritarian regime, cyber-activists displayed remarkable ingenuity in leveraging technology to disseminate information, counter propaganda, and maintain communication in the face of adversity during the early stages of the revolution. Their efforts played a crucial role in shaping the narrative of the Syrian revolution and highlighting the power of digital activism in contemporary conflicts. Intelligence branches started monitoring cyber activities extensively. To evade surveillance, activists use aliases, protective software, and maintain separate online accounts for activism. Despite these measures, activists frequently face arrests for minor online activities, with intelligence services using compromised accounts to trap others. Advanced technical individuals are particularly targeted and end up on official wanted lists. On the other hand, as the Syrian conflict intensified with increased arrests, killings, and international silence, cyber-activism began to wane, shifting the focus towards real-world activism and humanitarian efforts. Additionally, the lack of institutional support, high operational costs, and infiltration of state-backed cyber groups by the regime further accelerated the decline of cyber activism despite the support of international independent hacktivists groups. These groups are explained in detail in the next chapter.

CHAPTER VI

6. CYBERNETIC GROUPS: MANOEUVRING OPERATIONS IN SYRIAN CYBERSPACE

With many areas falling outside the regime's control and relying on alternatives to the local Internet to access the Internet, the government has moved to a new method of infiltrating the work of activists. The regime started the deployment of trained allies on hacking techniques and cyber-attacks over the social media website. This technique turned the cyber domain into a real battlefield with activists, as the Internet became full of ambushes and traps, and many social media pages and websites were hacked and closed.

Wilhelmsen, who studied the use of hacking by non-state groups, mentioned that the main objective of non-state cyber-actors, including pro- and anti-government, was subversion, meaning to hack social media accounts, websites, and local networks to post their narrative or leak valuable data to embarrass the opponent. These cyber groups used guerrilla tactics in cyberspace. These groups varied in size and professionalism, and their efficiency relied on their ability to take collective actions in an organized way and have the proper resources for this. Their operations could be in three categories: one attack carried out by one person or small group of people, a limited number of attacks by small groups, and attacks coordinated with international actors (Wilhelmsen, 2014).

6.1. Anti-Regime Groups

According to Racicot, cyber conflict in Syria has evolved in parallel with the field conflict. hacktivists and tech-savvy civilians are in the frontlines of this cyber conflict, employing their digital fluency and computing competencies to engage and support their cause in cyberspace (Racicot, 2015). It was clearly the cyberspace winner as their narrative dominated social media networks.

Wilhelmsen revealed that several hacktivist groups operated independently without coordination and were only known after a successful cyber operation, mainly web defacement. One group, the Syrian Revolution - Electronic Suite, successfully hacked the Russian Presidential Envoy's webpage. Another group, the "Hackers of the Syrian Revolution," breached various institutions but did not leverage these breaches beyond showcasing their abilities and posting the narrative of opposition. They leaked a list of

those wanted for arrest from the General Security Department. However, the cyber-attacks launched by these hacktivists were not considered sophisticated attacks. They were limited to DDoS against governmental websites, hijacking social media accounts, and defacement.

As in the real world, the anti-regime faced challenges due to internal divisions, the inability to collaborate and coordinate effectively, and the lack of funds and support. The regime's surveillance, censorship, and brutal disruption capabilities supported by allies, pose significant challenges in forming a unified and professionalized force within Syria cyber domain. The cyberspace environment hinders the efficiency of hacktivists groups, impedes developing a unified and consistent narrative, and makes it challenging to launch united cyber campaigns. Moreover, unreliable electricity and internet access obstruct the efforts of these hackers, while the physical conflict results in the loss of human capital. Additionally, the worsening situation in the conflict prompts supporters to direct their resources on humanitarian aid or military. Consequently, cyber-activists sought support abroad, by contacting international hacktivists forums.

6.1.1. Telecommix: Hacktivists fighting for the flow of information.

Telecommix is a multi-national, decentralized, unorganized group of cyber-activists with solid technical skills and belief in freedom of speech. They have gathered for the first time against a proposed EU legislation restricting Internet access for people who download copyrighted materials. Telecommix employed their expertise in helping Syrian activists by providing techniques to overcome and avoid government censorship and protect their anonymity. They also offered support in communication and material securely sharing over the network. For example, they created a video portal for activists to upload their event recordings securely (Khamis et al., 2012). Taylor Owen quotes one of Telecommix's members that they are “motivated by a radical passion for freedom” and “drawn together by the desire to have an Internet adventure, to see what free communication can do in the lives of ordinary people.” (Owen,2015). Reflet journal Article on Syria censorship stated that Telecommix supported Syrian mainly in two aspects: (1) Raise awareness among cyber-activists in the use of safe internet access by using anonymized web browsing software such as ‘Tor’ and ensure using safe URLs with HTTPs to ensure that the data is being transmitted safe to the website and (2) Assist in data transmission out of the country anonymously, such as ensuring videos recordings of

events or personal testimonies, is leave the country while safeguarding the anonymity of those disclosing the information (Kheops, 2011).

From this technical standpoint, the governmental network in Syria lacked cyber protection, which made it easily vulnerable to attack. While scanning the Syrian cyberspace, Telecommix hacktivists identified 5,000 unsecured home routers and alerted the owners about the risk of state surveillance. Additionally, they came across records indicating the online activities of numerous Syrians, encompassing their locations, visited websites, and complete content details. These findings were connected to one of the monitoring devices utilized by the regime, sourced from the American company Blue Coat Systems.

6.1.2. Anonymous; new disruptive power

It is another decentralized, unorganized, and structureless group that began its activity by combating any censorship on the Internet. It represents the development of political activity and expression of opinion without the need to go to the street, participate in demonstrations, and resort to violence to achieve its goals. It represents a clear example of cyber-activisms that could disrupt a wide range of once-powerful 21st-century institutions, not just international affairs. Owen quotes Yochai Benkler, a professor at Harvard University's Berkman Center for Internet and Society, who wrote in 2012 in Foreign Affairs that "Anonymous illustrates one of the fundamental new aspects of power in a networked, democratic society: individuals are vastly more effective and less susceptible to manipulation, control, and repression by traditional authority than they were even a decade ago. At one end is the hope that technology can make our social and governance systems more efficient. On the other is a desire to burn down the house—to take down the state" (Owen, 2015).

The pervasive, decentralized, and collaborative model of Anonymous has enabled coordinated attacks from different regions worldwide and, in particular, has provided an excellent platform for coordinating Distributed Denial of Service (DDoS) attacks. Knowing and reaching its members was also tricky because they spread and worked anonymously (Baezner & Robin, 2017).

Amjad Baiazy said that Anonymous started its operations against the Syrian regime because of the Internet blockade in Syria (Baiazy, n.d.). Anonymous focused on cyber-attacks targeting the websites of government ministries and institutions. They revealed the weak security of the Syrian government's network and took advantage of that

to hack its websites and publish a narrative contrary to the regime's narrative. These attacks caused some confusion for the regime, especially at the beginning of the events in Syria, where government propaganda was based on denying the existence of any protests. This created a sense of confusion among the general public regarding the actual events unfolding on the ground, and helped mobilize counterpropaganda, and demonstrated the regime's weakness in controlling its websites. (Rey, 2017)

Syrian Files was one of the fabulous operations by Anonymous and was revealed in June 2012. At this date, Wikileaks started publishing a collection of more than two million emails from Syrian political figures and international institutions between August 2006 and March 2012(Racicot, 2015). Syrian files provided clear evidence of Western hypocrisy as they shed light on the relationship between the Syrian government and the United States. Anonymous stated they had put much effort and worked for many days to breach computer servers in Syria and highlighted that the available data was so extensive that its download took several weeks.

Many other small groups and individuals were available in cyberspace to support activists safely surfing the internet and overcoming the issues. These groups were not organized or titled in order not to be recognized by the regime and attacked. They were able to hijack the website of the Syrian parliament and take down the 'Al Donya' website, which is a pro-regime TV station, using (a DDoS) distribution denial of service attack.

A prominent incident by an unknown hacktivist group was the successful hacking of the inbox of Syrian President Bashar Al-Assad. Over three thousand emails, dated between May 2011 and February 2012, were breached, and security concerns were raised. This was a massive scandal since the messages included many private communications between the president and his wife, as well as jokes and inappropriate photos (Baezner & Robin, 2017).

The regime noticed the danger of hacktivist groups and treated them as a real threat, so it began working to suppress their strategy through two things. First, it targeted Internet activists more precisely. And deploying counter teams on the Internet that use the same techniques and carry out counterattacks.

6.2. State-backed Cyber Groups

Despite the iron grip imposed by the regime on the cyber sphere, which we reviewed previously, which includes specifying that any entry and exit of data must be

carried out by the Syrian Telecommunications Company, as well as the installation of Internet monitoring devices, legal penalties for Internet crimes, and the role of intelligence in monitoring all types of wired and wireless communications, However, the success of cyber-attacks carried out by activists, especially groups from outside the country, pushed the regime to rely on third-party groups. Although these groups claimed that the state did not support them, they had a very close relationship with the state agencies, especially the intelligence services, and received much support from them.

Although the names of small groups that claimed to be independent and supported the regime's narrative appeared on the Internet and made some intrusions into accounts and websites affiliated with the opposition, it later became clear that these groups were individuals with technical expertise and a direct connection to the state. They later formed what was known as the Syrian Electronic Army (SEA). From these groups, the name SMT, or the Syrian Malware Team, and the Shadow, which later turned out to be a single person who assumed leadership of the Syrian Electronic Army, was later placed on the US sanctions list.

The shadow and SMT used almost the same cyber-attack techniques, distributing malware resembling genuine software through attachment to an email or by posting malicious links on social media, leading to the installation of software that can infiltrate a target's phone or personal computer, extracting files, passwords, location data, and contact lists. According to an expert, upon download, it seizes control, enabling actions such as activating the phone's camera and file extraction (Clinic et al., 2021). After a few months of the cyber-crisis, these two groups merged into the Syrian Electronic Army, and their names are no longer mentioned.

6.2.1. Syrian Electronic Army (SEA)

Mark Barrow best described the Syrian Electronic Army as "the state's de facto digital military service" (Barrow, 2022, p.3). It is believed that it was the state's response to counter the domination of the opposition narrative in cyberspace. SEA is a team that is close to the Syrian regime, and their main aim was to disrupt, hack, and deface any website or social media page -whether local or international- that publishes the narrative of opposition or shares media materials related to political and military events in Syria. In June 2011, Bashar al-Assad thanked SEA publicly acknowledging its existence, and their efficiency in becoming a "force within cyberspace" as mentioned in one of his speeches (Rey, 2017).

SEA's early days showed limitations in their technical skills and hacking abilities. Their objective to change the narrative of opposition pushed them to target any social media page or website, mainly focused on Facebook, and post aggressive comments and photos of the Syrian president. Statements like “leave us alone, we love Bashar” and “stay away from us, we love Syria” were posted in coordinated ways on Facebook pages of many international organizations, media, and political figures, such as pages of the European Union, Human Rights Watch, Aljazeera news agency former Presidents of France Sarkozy, former U.S. President Barack Obama and many other international figures (Margaret Weiss, 2012). Consequently, opposition hacktivist groups closed all SEA Facebook pages, and SEA lost the social media battle by mid-2012 and almost lost its presence on Facebook (Shehabat, 2013). After that, SEA focused on publishing on their website, which was registered under a domain on Syrian Computer Society servers (Margaret Weiss, 2012). Afterward, they transferred to the official Syrian STE servers under the domain (SEA.sy) (Wilhelmsen, 2014). However, this website was blocked due to a security threat under the Enterprise Malware category. September 2011 was the first realized attack by SEA. The group hijacked the Harvard University website and posted regime narratives and photos on the homepage (Shehabat, 2013).

In late 2012, the Syrian Electronic Army began to show more outstanding capabilities in online activism through its success in penetrating activists' websites and Facebook pages. Vivi Wilhelmsen stated in their study that SEA activists underwent training in Dubai supported by Russia and received monthly salaries from Rami Makhlouf, the CEO of Syriatel and the cousin of the Syrian President. Digital Dominion report argued that while older SEAs were using unsophisticated techniques that serve as warnings to the user, the new SEA started using malware, which run as a professional and authenticated program. Consequently, victims are less likely to detect any monitoring or compromise of sensitive information, remaining unaware of the intrusion.

Abdulkadir, who was a student at Informatics Engineering in Damascus, said: “A group of regime supporters were receiving salaries from the Syrian Students' Union, which affiliated with the Baath Party, and some were members of the administrative body at the Information Technology Engineering College in Damascus university. They were provided with iPhones and laptops by regime loyalists to use in spreading regime propaganda on social media and disrupting the revolution narrative. The funny part is they chose iPhones because service provider reports indicated that certain Twitter hashtags were retweeted from iPhones. They assumed that using Twitter required

iPhones, while Facebook was used on laptops, thinking each platform operated on a specific device; they were so stupid. Their main task was to create false narratives on social media. They would deny the occurrence of protests; for example, someone would say, “I am from Daraa; it is quiet today. There were no bombs or shelling” while the regime is bombing. Then these groups were part of the Syrian electronic army”.

Operations by SEA

Wilhelmsen estimated the total number of reported cyberattacks by SEA to be about 80. As we mentioned previously, the most sophisticated attacks occurred between 2013 and 2014, emphasizing that SEA was trained in hacking before 2013. During this period, SEA started using phishing, in which they target large groups of people - by sending emails, for example - with links to fake updates for valuable applications such as WhatsApp and Telegram, embedded with sophisticated malware capable of stealing many private information from the victim device, including location and intercepting communications without leaving any warning.

In 2013, SEA employed this phishing technique to hack Associated Press staff members and access AP's Twitter account. SEA hackers then took control of the Twitter account of Associate Press to disseminate fake news stating: “Breaking: Two Explosions in the White House and Barack Obama is injured.” Consequently, this tweet led to a staggering loss of $140 billion in the stock market, which was recovered after revealing the facts behind this news (Grohe, 2015).

In the same year, SEA members infiltrated the messaging app "Tango" and extracted millions of individuals' personal phone numbers, email addresses, and contact details. Tango refrained from detailing the complete scope of the information accessed or the method used by SEA to acquire private data. After acquiring this data from Tango, the SEA declared that data would be handed over to the Syrian regime. This data contained much information that could lead to identifying opposition activists' private personal information, which could harm their lives (Clinic et al., 2021).

Digital Dominions study quoted one of the experts describing the malware used in these attacks: “The minute you download this, it will take control over your computer, can turn on your phone camera, and can extract files.” The sophistication of this malware emphasizes speculation that it might have been developed by Russia or Iran or with their support (Clinic et al., 2021).

Moreover, SEA started using spear phishing techniques, in which the hacker targets specific targets to hack activists and armed group leaders, disclose sensitive

information such as meeting and military operations locations, and intercept their communications. SEA used fake profiles on Skype and Facebook, and frequently, they assumed the identities of women who appeared supportive of the Syrian revolution. After they establish a conversation with the victim, they deploy the malware by sharing links to a video or photos, which results in taking control of data on the victim's device(Clinic et al., 2021).

In another context, the Syrian Electronic Army also re-created its Facebook page and began exploiting Facebook's policy to report on rebel Facebook accounts, which often use fictitious names – Facebook policy only allows real names - as well as news pages affiliated with the opposition that publish videos of the regime's brutal repression, as well as those that publish news about Free Syrian Army operations against the government, as they violate Facebook policy. As of mid-2020, Facebook has deleted approximately 10,000 opposition pages and accounts belonging to anti-regime groups, including pages with millions of followers, such as "We are all Hamza Al-khatib." This ultimately fed into the overall goal of the Syrian Electronic Army, which is to disrupt the anti-regime narrative in cyberspace (Clinic et al., 2021).

By late 2013, SEA members started using hacking techniques to make personal profit, which are recognized as cybercriminal attacks. The Shadow, th3pr1023, and Pierre Romar, the famous members and co-founders of SEA, whose name was revealed by the FBI office to be Firass Dardar and Ahamd Agha and Peter Romar, started to attack private business companies, including online Gaming and web-hosting companies, gaining unauthorized access and information, and demanding payments ranged from five hundred to three hundred thousand euros to give access back to the companies.

6.2.2. Group 5

Citizen Lab research centre, which focuses on cyber espionage, surveillance, and digital rights investigations, published a research report 2016 revealing a new cyber group operating in Syria's cyber domain. This group was revealed after analysis of many emails disseminating the narrative of opposition and sent from unknown human rights organizations. One of these emails, for example, was titled "Assad Crimes" and sent from an email registered on a domain called "assadcrimes.info." the email contains a PowerPoint Slideshow document with .pptx extension containing many unstructured political information mostly about Iranian crimes against Saudi Arabia. After examining the file by Citizen Lab, it was found that it downloads malware onto the victim's device. The website hosted on "assadcrimes.info" included anti-regime content and links from

Tal Almallouhi blogs – the well-known detained cyber-activist. Also, the websites contained links to PowerPoint slideshows with the same embedded malware and other malicious links. Moreover, the website contained other malware for mobile phones with the Android operating system.

After detailed analysis by experts, Citizen lab researchers argued that “Group 5” was believed to be an Iranian-based cyber group trying to jeopardize opposition communications. Although the evidence analysed by experts is insufficient to state the existence of a direct relationship with the Iranian government, the sympathy of many in that country for the Assad regime and Iranian military support supports the hypothesis that this group is operating from Iran.

There is no information about the operations carried out by this group other than the malicious mail that the experts analysed and which was sent to the mail of one of the well-known figures in the Syrian opposition.

6.2.3. Cyber Lebanese Group

A report published by FireEye, an international cybersecurity company, indicated a group operating from Lebanon carrying out attacks on Syrian opposition accounts using spear-phishing. While talking through messaging programs with the victim, a female character sends malicious links that lead to malware downloading on the victim’s device. The report also linked this group to Hezbollah's Islamic Resistance. FireEye report mentions that during the investigation of this group, they came out with a leaked Syrian intelligence memo announcing a 3-days training in Lebanon for social media activists, which includes: (1) establishment of an "Electronic Army" to infiltrate the computers, websites, and online accounts of Syrian activists. (2) Establishing social media profiles aligned with opposition interests to spread false information, initiate accusations, and foster conflict among opposition members within and outside Syria. (3) Employing women to lure and trap opposition members and activists via social media platforms like Skype and Facebook (Regalado et al., 2015). This confirms the hypothesis that members of the Syrian Electronic Army received training outside Syria and their direct relationship with the Syrian regime.

6.3. Targets and Vulnerabilities

We can realize three main phases of the operations carried out by state-affiliated groups in the cyber domain, and they are linked to three temporal stages:

The first phase extends approximately from the beginning of the crisis in mid-2011 to mid-2012. These groups targeted anti-regime narratives on social media and international news agencies' websites during this phase. Despite its success in penetrating a few websites, such as the Harvard University website, the opposition narrative remained dominant and most accessible for several reasons, including the success of the opposition groups in closing the Syrian Electronic Army page on Facebook many times. This phase sheds light on these groups' limitations and lack of experience. During this phase, the cyber groups used social media accounts to post comments widely and randomly on the pages of international influencers, as well as the social media pages of international news agencies. They also used phishing with unsophisticated malware to target many news agency employees. They emailed opposition activists by seeding malicious links while commenting on Facebook pages.

The second phase started from late 2012 to the beginning of 2014 when the attacks carried out by state-backed groups notably developed as they began to use professional hacking strategies by using advanced malware and implanting them in updates or software applications that do not give any warning notification when they are downloaded onto the victim's device. It also clearly used two techniques, phishing, when attempting to penetrate international news pages and websites to create confusion, spread the regime's narrative, and demonstrate its capabilities in controlling the cyber domain. Likewise, Spear phishing attacks well-known opposition activists and attempts to steal data to know their locations, movements, and on-ground plans. It uses it to hand it to state forces to liquidate or thwart their activity. This was done by using female avatars on Skype, through which they created a relationship of trust with the victim, where the female attacker sent a picture through an executable file. When the image is opened, a malicious program is downloaded onto the victim's device, which takes over all the data.

FireEye report published an analysis of a set of stolen data obtained from a state-backed cyber group. The breach involved sensitive information across several crucial areas: insights into Syrian opposition, including **Sensitive military information**; available weapons and positions of fighting groups; lists of members and personal information of these fighting groups; weapons and serial numbers each man carried; their

blood types, and their phone numbers. **Political information** like discussions, political structure documents, and diaspora alliances. **Humanitarian data**, such as needs assessments, refugee camp structures and locations, aid distribution plans, and personal information of refugees applying for assistance, like recipient lists and ID card scans. Additionally, breached documents encompassed **media-related content**, such as casualty lists and reports on human rights abuses, providing a comprehensive view of compromised information across politics, humanitarian aid, refugee details, and media communications (Regalado et al., 2015).

Third phase: By late 2013 and after 2014, members of these groups benefited from the experiences they gained to achieve personal gains and turned into cybercriminals. They attacked private companies, stole their data and log-in credentials to their systems, paralyzed their work, and demanded money in exchange for returning the data and access information to the victim.

6.4. International Response to the State-backed Operations

On the other hand, since the outbreak of the civil unrest in 2011, The U.S. Department of State and the European Union have been implementing sanctions targeting various sectors and individuals or entities deemed responsible for human rights abuses, supporting the Syrian regime, or contributing to the conflict's perpetuation. The sanctions encompass multiple aspects, including restrictions on the export of specific equipment and technologies. Entities and individuals within the telecommunication sector have been subject to sanctions. For example, in 2012, The Minister of Telecommunication was added to the sanctions list of EU, due to providing direction for controlling web content and implementing surveillance systems that censor freedom of speech.

In another context, three members of the Syrian Electronic Army were listed on the most wanted list by the U.S. Federal Bureau of Investigation (FBI) in 2015. Firass Dardar, Ahamd Agha, and Peter Romar were accused of committing dozens of cyber-attacks against United States government entities, media agencies, and private business companies using their nicknames under SEA. Peter Romar was arrested in Germany and extradited to the U.S. and is facing five years in prison, While Ahmad Agha and Firass Dardar have not been captured (Virginia, 2022).

To sum up, in response to the Syrian government's attempts to control the internet in areas outside its control, cyber conflict intensified, turning the digital realm into a

battleground. Both pro- and anti-government cyber-actors engaged in subversive tactics, using guerrilla-style cyber-attacks to assert their narratives. The Syrian regime, facing challenges from activist cyber-attacks, relied on state-backed cyber groups like the Syrian Electronic Army (SEA). SEA evolved by 2013-2014, receiving international support from Russia and employing advanced hacking techniques like phishing and spear phishing. Alongside SEA, other groups like "Group 5" from Iran and the Cyber Lebanese Group linked to Hezbollah, operated to disrupt opposition communications. These state-affiliated cyber operations spanned three phases, targeting anti-regime narratives, employing professional hacking strategies, and eventually engaging in cybercriminal activities for personal gains, resulting in significant data breaches across military, political, humanitarian, and media sectors. On the other hand, although hacktivist groups showcased their abilities through web defacements and breaches, they faced challenges due to internal divisions, lack of coordination, and limited resources. Internationally, the only response to from the U.S. and the EU to the cyber operations by regime-backed cyber groups was imposing sanctions on individuals and entities involved in human rights abuses. Accordingly, several SEA members have been listed on the FBI's most wanted list, with some facing legal consequences.

CHAPTER VII

7. CONCLUSION & RECOMMENDATIONS

This study provides a comprehensive overview of the cyber landscape in Syria, starting from the introduction of the Internet in 1997. It focuses on cyber activity during the Syrian revolution in mid-2011 when digital engagement played a crucial role in spreading awareness and amplifying voices in a challenging and highly controlled environment. However, the study acknowledges the inherent risks and limitations involved in such activities in Syria.

The study establishes a conceptual framework to distinguish between cyber activity, cyber warfare, and cybercrime. It also categorizes cyber gangs and activist groups and applies this framework to Syria's cyber landscape. The study maps the entities providing cyber services, decision-making institutions, and the regime's involvement through security services and tools used for control.

The Syrian regime has significant control over the cyber domain, implementing multi-layered censorship, including governance, monitoring equipment, legal, intelligence, and state-supported cyber groups. Despite this, cyber activists navigate within limited freedom using anonymity tools, accessing alternative networks in neighboring countries, and receiving support from international cyber entities.

The study established a conceptual framework to delineate cyber activity, distinguishing it from cyberwarfare and cybercrime. It emphasized that cyber activity involves substantive actions beyond mere social media engagement and delineated between cyber gangs and activist groups pursuing political or social change.

We applied this theoretical framework to Syria's cyber landscape, which involved mapping the entities providing cyber services, decision-making institutions, and the regime's involvement through security services and tools used for control. This mapping facilitated an understanding of Syrian cyber activists' challenges, opportunities, and constraints. The study also cataloged professional cyber groups, delineating their impact on the trajectory of cyber activity.

The Syrian regime wielded significant control over the cyber domain, implementing multi-layered censorship:

1. Governance Layer: The Syrian Telecommunications Company monopolized access to the global network, regulating service providers and making technological decisions through its affiliated directorates.
2. Surveillance Infrastructure Layer: Working with international firms, the regime set up comprehensive monitoring systems for internet and telephone activities. This layer enabled data collection, censorship of content, identification of individuals, and control over communication access.
3. Legal Framework Layer: The Cybercrime Law imposed strict restrictions on online expression and mandated content retention. It criminalized the dissemination of false information or criticism against the state.
4. Intelligence Apparatus Layer: Security branches used the Syrian Telecommunications Company to access data, representing the regime's operational arm in the cyber sphere.
5. State-supported Cyber Groups: Entities like the Syrian Electronic Army aimed to counter opposition discourse, launch cyber attacks, spy on activists, and steal data.

From mid-2011 to late 2013, cyber activists briefly controlled the cyber world in Syria due to the government's incompetence and corporate withdrawals amidst sanctions. They used anonymity tools and alternative networks in neighbouring countries to navigate within limited freedom. International cyber entities such as Anonymous and Telecommix supported them during their activities, which facilitated information exchange, provided an alternative global narrative, and overcame geographical and ideological barriers. However, due to increased attacks on dissenting voices, preserving their gains required a strategic shift towards documentation. Weaknesses in cyber activity included arbitrary arrests, institutional disorganization, reliance on individual donations, lack of global support, and limited impact due to Syria's non-reliance on cyber networks for government or military operations. Cyber activists' ideological influence was limited, and many transitioned to humanitarian efforts amidst the crisis. Cyberactivism extended the reach and impact of the Syrian revolution significantly. Future studies should examine cyber activity in areas beyond regime control and evaluate the effect of Russian intervention on cyber capabilities.

Studying cyberactivism in Syria is a dynamic and complex field that intersects with political, security, and technological dimensions, given the evolving nature of conflict, politics, and digital landscapes. Implications of Russian intervention in the

conflict add another layer of complexity to the field of cyberactivism research. Moreover, The change of power over areas like North West Syria (NWS) and North East Syria (NES) has indeed had a significant impact on the structure of the cyber landscape in the country. These changes in territorial control, governance, administration, and Russian intervention have reshaped the dynamics of digital activism, information dissemination, and online communication in the respective regions.

Furthermore, comparative studies on cyber-activism in countries during Arap spring, offer valuable insights into the diverse strategies, dynamics, challenges, and opportunities shaping online activism across different contexts. By examining the similarities and differences in the cyber landscapes, challenges experiences, practices, and impacts of cyberactivism in various Middle Eastern countries, researchers can gain a deeper understanding of the complex interplay between technology, politics, and society.

On the other hand, the Israeli military has reportedly conducted multiple cyber-related operations in Syria as part of its broader strategy to counter threats posed by Iran, Hezbollah, and other actors in the region. These cyber operations have targeted critical infrastructure and military bases associated with the Syrian government, Iranian forces, and allied militias.

By addressing these areas, future research on cyber-activism in Syria can provide valuable insights and contribute to a more nuanced understanding of how digital technologies are being leveraged to challenge authoritarianism, promote human rights, and facilitate civic engagement in one of the most complex and contested environments in the world today.

"Without cyberspace, the revolution would have struggled—live streaming aided in amplifying the demonstrations." -Samer.

"Without cyberspace, I do not think the revolution would have spread. It facilitated the rapid spread of news, crucial in mobilizing other areas before they could be suppressed and silenced." -Abdulkadir.

"Without sharing numerous video clips and news on social media, many events would have escaped global attention. Social media acted as the carrier that delivered these details. I cannot imagine how they would have spread otherwise. How else could the voice have reached the world?" - Ahmad

"I believe the images being transmitted were the cause of some of these actions from some countries. The shared media were shocking; the existing security grip made some disbelieve that people were protesting." – Wafi.

REFERENCES

AlJazeera, (2020, May 19). Syrian government orders seizure of assets of Rami Makhlouf. Al Jazeera. Retrieved October 9, 2023, from https://www.aljazeera.com/economy/2020/5/19/syrian-government-orders-seizure-of-assets-of-rami-makhlouf

Al-Saqaf, W. (2016). Internet Censorship Circumvention Tools: Escaping the Control of the Syrian Regime. Media and Communication, 4, 39–50. https://doi.org/10.17645/mac.v4i1.357

Amnesty International. (2011). Amnesty International public statement.

Applegate, S. (2011). Cyber-militias and Political Hackers: Use of Irregular Forces in Cyberwarfare. IEEE Security & Privacy, 9, 16–22. https://doi.org/10.1109/MSP.2011.46

Baiazy, A. (n.d.). Syria's cyber war.

Barrow, M. (2022). Challenging Information Control with Communication Technologies in Syria. E-International Relations. https://www.e-ir.info/2022/04/26/challenging-information-control-with-communication-technologies-in-syria/

Biswas, M., & Sipes, C. (2014). Social Media in Syria's Uprising and Post-Revolution Libya: An Analysis of Activists' and Blogger's Online Engagement. Arab Media & Society.

CHAMPAGNE - KITETOA, A. (2014). Network surveillance: Qosmos, a tool provider for Syria's leader al-Assad. https://reflets.info/articles/network-surveillance-qosmos-a-tool-provider-for-syria-s-leader-al-assad

Chang, W.-Y., & Lee, W.-T. (2006). Cyberactivism and political empowerment in civil society: A comparative analysis of Korean cases. Korea Journal, 46, 136–167.

Clinic, U. I. C. J. M. L. S. I. H. R., Guruli, N., & Samaro, D. (2021). Digital Dominion: how the Syrian regime's mass digital surveillance violates human rights.

Cisco newsroom. (2020b, February 18). New Cisco annual Internet report forecasts 5G to support more than 10% of global mobile connections by 2023. Retrieved November 7, 2023, from https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2020/m02/new-cisco-annual-internet-report-forecasts-5g-to-support-more-than-10-of-global-mobile-connections-by-2023.html

De Angelis, E., & Badran, Y. (2016). Interacting in a context of war: Communication Spaces in Idlib. Confluences Méditerranée, 99, 149–160. https://doi.org/10.3917/come.099.0149

Freedom House. (2020). Freedom On The Net.

Göksun, Y. (2014). Cyberactivism in Syria's War How Syrian Bloggers Use Internet for Political Activism.

Grohe, E. (2015). The cyber dimensions of the Syrian Civil War: Implications for future conflict. https://doi.org/10.21236/ada620195

Hennefer, A. N. (2013). Cyberactivism: A generational comparison of digital activism. In University of Nevada, Reno.

Hiba Mohammed. (2019, July 19). روسيا تعيد هيكلة أجهزة استخبارات النظام السوري: تسريب أمنيّ. Alquds.Co.Uk. Retrieved November 9, 2023, from

https://www.alquds.co.uk/%D8%AA%D8%B3%D8%B1%D9%8A%D8%A8-%D8%A3%D9%85%D9%86%D9%8A%D9%91-%D8%B1%D9%88%D8%B3%D9%8A%D8%A7-%D8%AA%D8%B9%D9%8A%D8%AF-%D9%87%D9%8A%D9%83%D9%84%D8%A9-%D8%A3%D8%AC%D9%87%D8%B2%D8%A9-%D8%A7%D8%B3%D8%AA/

John Leyden. (2011, September 21). UK firm denies supplying spyware to Mubarak's secret police. The Register.

Khamis, S. (2017). Revisiting Cyberactivism Six Years after the Arab Spring: Potentials, Limitations and Future Prospects. In Springer eBooks (pp. 3–19). https://doi.org/10.1007/978-3-319-65771-4_1

Khamis, S., Gold, P., & Vaughn, K. (2012). Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies. Arab Media & Society, 15.

Khamis, S., & Vaughn, K. (2011). Cyberactivism in the Egyptian Revolution: How Civic Engagement and Citizen Journalism Tilted the Balance.

Khamis, S., & Vaughn, K. (2012). We Are All Khaled Said: The Potentials and Limitations of Cyberactivism in Triggering Public Mobilization and Promoting Political Change. Journal of Arab & Muslim Media Research, 4, 145–163. https://doi.org/10.1386/jammr.4.2-3.145_1

Kharroub, T. (2015). Cyberactivism in the Middle East: Six potentials and six limitations of new media technologies in democratization. Arab Center Washington DC. Retrieved April 18, 2023, from https://arabcenterdc.org/resource/cyberactivism-in-the-middle-east-six-potentials-and-six-limitations-of-new-media-technologies-in-democratization/

Kheops. (2011). #OpSyria: When the Internet does not let citizens down. Reflects.

Lee, B. (n.d.). The impact of cyber capabilities in the Syrian Civil War | Small Wars Journal. Retrieved April 12, 2023, from https://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war

Maen Tallaa. (2016). The Syrian Security Services and the Need for Structural and Functional Change.

Mansour, F. A. (n.d.). Cyber-activism: Engendering Political Subjects within New Logics of Resistance in Contemporary Egypt and Yemen. Retrieved March 8, 2023, from https://fount.aucegypt.edu/etds/1353/

Margaret Weiss. (2012). Assad's Secretive Cyber Force.

McCaughey, M., & Ayers, M. D. (2003). Cyberactivism: Online Activism in Theory and Practice. Psychology Press.

Mehan, J. E. (2015). Cyberwar, Cyberterror, cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger. IT Governance Ltd.

MoCT. (2013). المهام والأهداف. (n.d.). وزارة الاتصالات والتقانة. Retrieved September 16, 2023, from https://www.moct.gov.sy/%D8%A7%D9%84%D9%88%D8%B2%D8%A7%D8%B1%D8%A9/%D8%A7%D9%84%D9%85%D9%87%D8%A7%D9%85-%D9%88%D8%A7%D9%84%D8%A3%D9%87%D8%AF%D8%A7%D9%81

Morgan Marquis-Boire, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton, & Greg Wiseman. (2013). Planet Blue Coat.

MTN Syria. (n.d.). Retrieved December 13, 2023, from https://en.wikipedia.org/wiki/MTN_Syria

NANS. (2017, December 6). https://nans.gov.sy/ar/page/establishment_of_the_national_network_se

Neumayer, C., & Raffl, C. (2008). Facebook for Global Protest: The Potential and Limits of Social Software for Grassroots Activism.

Owen, T. (2015). Disruptive power: The Crisis of the State in the Digital Age. In Oxford Studies in Digital Poli.

Powers, S., & O'Loughlin, B. (2015). The Syrian data glut: Rethinking the role of information in conflict. Media, War & Conflict, 8(2), 172–180. https://doi.org/10.1177/1750635215584286

Privacy International. (2016). Open season: Building Syria's Surveillance State.

Racicot, J. (2015). The Syrian Civil Conflict in the Cyber Environment. 10.13140/RG.2.1.2609.3287

Radsch, C. (2016). Cyberactivism and Citizen Journalism in Egypt, Digital Dissidence and Political Change.

Regalado, D., Villeneuve, N., & Scott Railton, J. (2015). Behind the syrian conflict's digital front lines.

Rey, M. (2017). Preventing a Mobilization from Spreading: Assad and the Electronic War (pp. 89–106).

RSF. (2014). Enemies of the Internet. https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf

Scmadmin. (2011). إعلام الإنترنت. Syrian Center for Media and Freedom of Expression. Retrieved December 8, 2023, from https://scm.bz/%D8%A7%D8%B9%D9%84%D8%A7%D9%85-%D8%A7%D9%84%D8%A7%D9%86%D8%AA%D8%B1%D9%86%D8%AA/

Shehabat, A. (2013). The social media cyber-war: the unfolding events in the Syrian revolution 2011. Global Media Journal, 6.

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. Journal of Military Studies, 4, 1–37. https://doi.org/10.1515/jms-2016-0184

SNHR. (n.d.). Syrian Security branches and Persons in charge.

SyTRA. (2018, January 10). Retrieved February 15, 2023, from https://sytpra.gov.sy/pages/%D8%A7%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA

Tounsi, M., & Zouai, M. (2022, October 5). Understanding Assad's New Cyber-Crackdown in Syria. https://timep.org/. Retrieved April 17, 2024, from https://timep.org/2022/10/05/understanding-assads-new-cyber-crackdown-in-syria/

VDC. (2013). Branch 215, Raid Brigade Military Intelligence Division - Damascus.

Virginia, U. S. D. C. for the E. D. of. (2022). Criminal Complaint (CaseNo. 1:15mj49). Office of Public Affairs U.S. Department of Justice.

Wilhelmsen, V. C. R. (2014). Soft War In Cyberspace How Syrian non-state actors use hacking to influence the conflict s battle of narratives. Retrieved February 10, 2023, from https://www.duo.uio.no/handle/10852/40273

ANNEX

Annex-1: Interview Questions

First: Interview questions for Cyber-activists

- Were you involved as an online activist during the Syrian revolution?
- Which platforms did you utilize and establish accounts on? When did you create your initial social media account, and what motivated you? Did you use your real name in your posts? What influenced this choice?
- What led to your selection of these platforms? What objectives were you pursuing?
- What specific field were you active in? Writing, raising awareness, news dissemination, cyber-attacks, or rallying people?
- What were the most significant challenges you encountered during your activities? Connectivity issues, expenses, surveillance?
- Are you acquainted with others who faced similar challenges?
- Do you still identify yourself as an online activist, and if so, why?
- Did you receive support, aid, or training from international or external sources?
- Were you engaged in activities with online groups? If so, what kind? Describe your involvement.
- Do you have any knowledge of the regime noticed your activities? If so, how did they respond?
- How did you execute attacks or operations?
- Did you possess any prior experience using social media or blogging for political purposes before the revolution?
- Do you view social media as a legitimate activity against authoritarian systems? To what extent do you consider social media activists genuine activists?
- When do you believe cyber activity began to decline in effectiveness in Syria? Why do you think so?
- Were you arrested during the revolution? Was it related to cyber activity? Were your social media accounts questioned? How did you react? Did the investigator's approach change due to your online activity?

- Did you participate in cyber operations or attacks on regime websites during the revolution? How did you get involved? What tools or platforms did you use, and what was your goal in participating?
- Do you believe you achieved your objectives through these operations? Yes or no, and how did you determine this?
- Are you currently involved in such operations? What motivates your continued engagement?
- What tools were utilized during the revolution, and what was the purpose of each tool?
- In your opinion, can members of active online groups share the same collective identity as face-to-face groups?
- Is cyber activity distinct from real-world political activity, or are they merely conflicts and demonstrations, possibly independent of real-world events?
- What became of the initiatives and groups in cyberspace that were launching attacks against the regime? Why did they cease?

أسئلة مقابلات الناشطين في المجال السيبراني

- هل كنت ناشطاً على الإنترنت خلال الثورة؟
- ما هي المنصات التي استخدمتها وأنشأت حسابات لك عليها،
- متى أنشأت أول حساب على السوشال ميديا؟ ولماذا؟ وهل كتبت باسمك الحقيقي؟ ولم؟
- لماذا اخترت هذه المنصات؟ ما الغاية من ذلك؟
- في أي مجال كنت نشطاً؟ الكتابة، رفع الوعي، نشر الأخبار، الهجمات، جمع الناس؟
- ما هي أكثر التحديات التي واجهتك أثناء نشاطك؟ الاتصال؟ التكاليف؟ المراقبة؟
- هل تعرف أي أحد واجه مثل هذه التحديات؟
- هل لا تزال تعتبر نفسك ناشط على الإنترنت ولماذا؟
- هل تلقيت أي مساعدة أو دعم أو تدريب من أي جهة دولية أو خارجية؟
- هل شاركت ضمن نشاطات مع مجموعات على الإنترنت؟ مثل من ؟ ماذا كان نشاطكم
- هل لديك معلومات إن واجه النظام نشاطكم؟ وكيف تم ذلك؟
- كيف كنتم تشنون الهجمات أو تقومون بالعمليات؟
- هل لديك أي خبرة سابقاً قبل الثورة باستخدام السوشال ميدييا أو البلوغننغ في نشاط سياسي
- هل تعتبر السوشال ميديا نشاط حقيقي ضد النظم لاستبدادية/ إلى أي مدى تعتبر الناشطين على السوشال ميديا ناشطين فعلياً؟
- متى تعتبرهم نشاطين فيسبوكيين أو مجرد أشخاص متكلمين ليس لهم تأثير خارج إطار السوشال ميديا؟
- متى تعتقد أن النشاط السيبراني بدأ يفقد قوته في سوريا؟ ولماذا؟

- هل تعرضت للاعتقال خلال الثورة؟ وهل كان ذلك بسبب النشاط السيبراني؟ هل تم سؤالك على حساباتك على السوشال ميديا؟ كيف تصرفت؟ وهل تغير تعاطي المحقق بسبب نشاطك الافتراضي؟
- هل شاركت في العمليات/الهجمات السيبرانية عى مواقع للنظام أثناء الثورة؟ كيف شاركت/بدأت؟ ما الأدوات/المنصات التي استخدمتها؟ ماذا كان الهدف من الانضمام؟
- هل تعتقد أنك وصلت إلى الهدف من خلال هذه العمليات؟ نعم / لا وكيف قمت بتقييم ذلك؟
- هل مازلتم تقومون بمثل هذه العمليات؟ لماذا ؟
- ما الأدوات التي استخدمتها أثناء الثورة وما فائدة كل أداة.
- برأيك هل يمكن للأعضاء المجموعات الناشطة عبر الإنترنت (الافتراضية) أن يتمتعوا بذات الهوية الجمعية التي تتمتع بها المجموعات التي تجتمع وجهاً لوجه؟
- هل بعكس النشاط السيبراني النشاط السياسي في العالم الحقيقي، أم أنها مجرد نزاعات واستعراضات وربما أعمال مستقلة تمامًا عما يجري على الواقع؟
- ماذا حدث لكل المبادرات والمجموعات في الفضاء الإلكتروني والتي كانت تشن هجمات ضد النظام؟ و لماذا؟

Second: Interview questions for Cyber-experts

- Which internet service provider or telecommunications company did you collaborate with?
- What was the duration and specific area of your involvement?
- Was the service provider directly linked to the global network? If so, which country was it connected to?
- What was the relationship between the company you worked with and entities like the Syrian Telecommunications Establishment (STE), intelligence branches, and the regulatory authority for communications?
- Are you familiar with any surveillance or censorship systems used by the government or the service provider you worked with? If so, could you describe these systems, their country of origin, the provider company, the selection process, and the criteria for choosing the company?
- Which institutions, security branches, or bodies primarily control the cyber domain, and what are the critical decision-making processes involved? For instance, how are requests made for monitoring specific individuals or blocking certain services?

- Can you identify companies or nations supporting the Syrian regime in surveillance and network management? What form did this support take?
- Have you noticed instances of monitoring of cyber activities during the revolution?
- Do you know anyone arrested for their online activities or their association with internet service providers?
- Were you involved in any cyber operations or attacks against government websites during the revolution? If so, how did you get involved, what tools or platforms did you use, and what was the purpose behind your participation?
- Do you believe that the cyber domain in Syria is under surveillance? If yes, why do you think so? And if there is monitoring, was it utilized to strengthen the regime's authority and suppress freedoms?

-

أسئلة مقابلات خبراء في المجال السيبراني في سوريا

- من هو مزود الخدمة الذي عملت معه؟ والفترة الزمنية؟ والقسم؟
- هل كان مزود الخدمة على اتصال مباشر مع الشبكة العالمية؟ مع أي دولة؟
- ما هي العلاقة مع STE والأفرع الامنية والهيئة الناظمة للاتصالات؟
- هل لديك علم بأنظمة مراقبة أو حجب تستخدمها الحكومة أو مزود الخدمة الذي كنت تعمل معه؟ ما هو هذا النظام؟ البلد المنشأ؟ ومن هي الشركة التي زودت به؟ وكيف تم اختياره واختيار الشركة؟
- ما هي الهيئات/ المؤسسات/الأفرع الأمنية المسيطرة على المجال السيبراني وما هي مؤسسات اتخاذ القرار الرئيسية؟ وكيف يتم ذلك؟ (مثلاً في حال طلب مراقبة شخص معين أو حجب خدمة معينة كيف يتم ذلك من ناحية الطلب؟
- هل تعرف أي شركات/دول كانت تدعم النظام في المراقبة وفي إدارة الشبكة؟ من هم؟ كيف كانوا يدعمون؟
- هل لديك أي حالات لاحظتها في مراقبة استخدام المجال السيبراني أثناء الثورة؟
- هل لديك أصدقاء تم اعتقالهم بسبب نشاطهم على الإنترنت؟ أو بسبب عملهم ضمن مزودات خدمة الإنترنت؟
- هل شاركت في العمليات/الهجمات السيبرانية على مواقع للنظام أثناء الثورة؟ كيف شاركت/بدأت؟ ما الأدوات/المنصات التي استخدمتها؟ ماذا كان الهدف من الانضمام؟
- هل تعتقد أن المجال السيبراني السايبر في سوريا مراقب بالكامل؟ نعم أو لا؟ ولماذا؟ وفي حال كانت نعم هل كانت تستخدم هذه المراقبة لتعزيز سلطة النظام وقمع الحريات؟

Annex-2: Syria's Internet Connection to the Global Network.

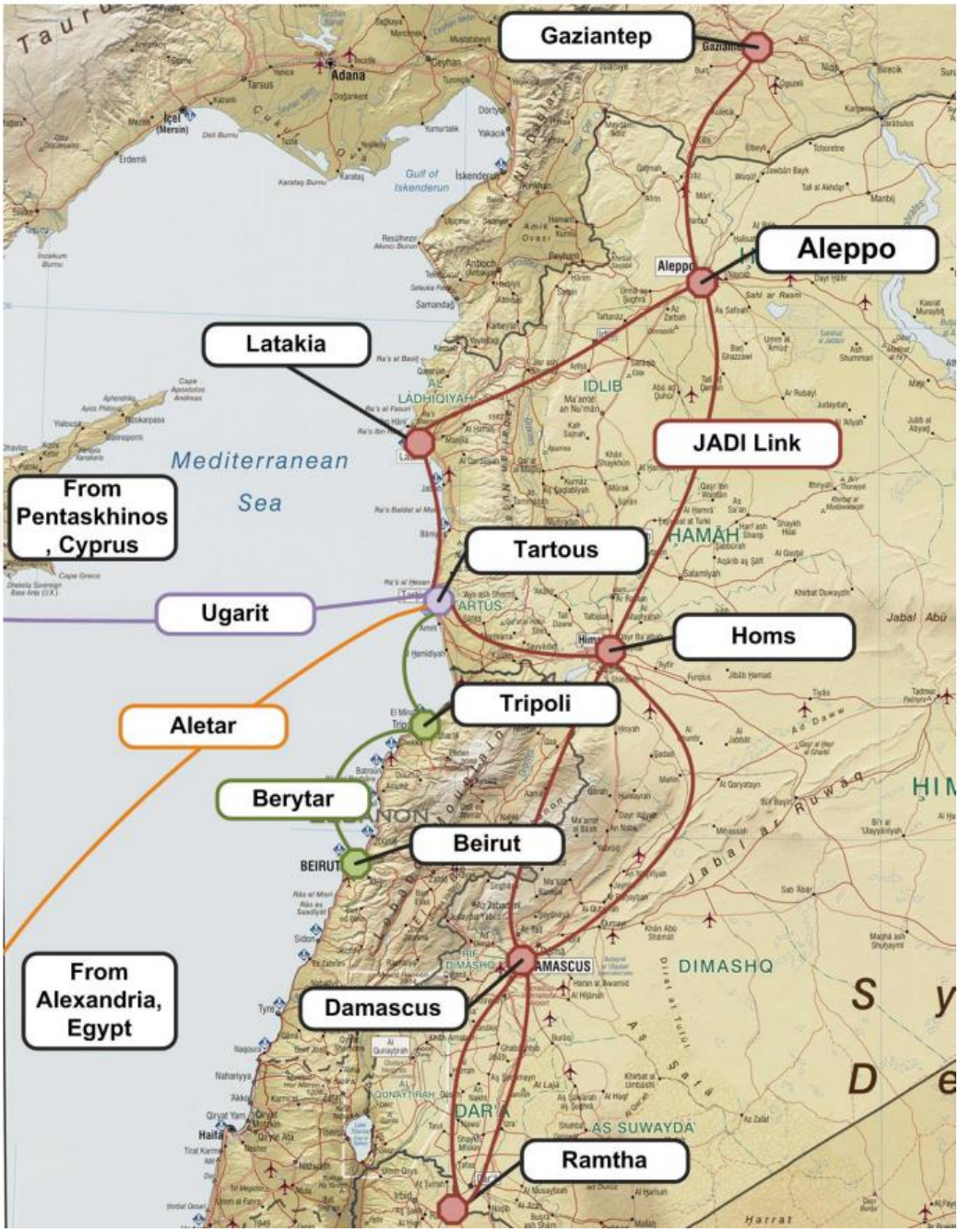

Figure 1- Syria's connection to the global network of three marine cables and one landline (JADI) (Racicot,2016)

RESUME

PERSONAL INFORMATION

Name and Surname: Iyad HELWANI

Nationality: Syrian

EDUCATION INFORMATION

Degree Name: Bachelor’s Degree in Software and Information Systems Engineering.

University: ALBAATH University, Homs, Syria.

Completion Year: 2007

WORK EXPERIENCES

Year	Institution	Position
2024-present	United Nations WFP	Program Policy Officer
2022-2024	United Nations WFP	IT Solutions Associate
2012-2022	Non-Governmental Organizations (SARD, MDM, OSRA, HIHFAD, AHF,AOUN)	Information Management, and Monitoring and Evaluation
2010-2012	Saudi Telecom Company (STC)	Software Development Engineer

PROFESSION

Data Management and Software Solutions for Social Science.

FOREIGN LANGUAGES

Arabic (Mother tongue), English (Fluent), Turkish (Upper Intermediate).