GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2024, 20:48, 239-263
DOI: 10.17752/guvenlikstrtj.1463912

Araştırma Makalesi
Research Article

Cyberactivism in Syria: Emergence, Transformation, Potentials, and Limitations

Suriye'de Siber Aktivizm: Ortaya Çıkışı, Dönüşümü, Potansiyeli ve Sınırlılıkları

Iyad HELWANI*

* Istanbul, Türkiye
e-mail: iyadhoo@yahoo.com
ORCID: 0000-0003-0232-7608

Geliş Tarihi / Submitted:
02.04.2024

Kabul Tarihi / Accepted:
20.07.2024

Abstract

The rise of the cyber domain and social media platforms has profoundly impacted the socio-political landscape in Syria, enabling cyber-activism to emerge as a potent force against authoritarian regimes. This qualitative research examines the evolution, impact, and challenges Syrian cyber-activists face, drawing from professional reports, interviews, and scholarly literature. While online platforms empower activists by facilitating mobilization and information dissemination, activists also face significant obstacles, including surveillance, censorship, and cyberattacks within a state-controlled digital environment. Despite these challenges, cyber-activism in Syria played a crucial role in shaping narratives, fostering solidarity, challenging the regime, influencing international perceptions, and highlighting the transformative potential of the cyber domain in repressive contexts.

Keywords: Cyberactivism, Hacktivist, Syria, Cyber Conflict, Arap Spring

Öz

Siber alanın ve sosyal medya platformlarının yükselişi, Suriye'deki sosyopolitik ortamı derinden etkilemiş ve siber aktivizmin otoriter rejimler karşı büyük bir güç olarak ortaya çıkmasını sağlamıştır. Bu nitel araştırma, profesyonel raporlardan, mülakatlardan ve akademik literatürden yararlanarak Suriyeli siber aktivistlerin gelişimini evrimini ve yaşadıkları zorlukları incelemektedir. Çevrimiçi platformlar harekete geçmeyi ve bilginin yayılmasını kolaylaştırırken, aktivistler aynı zamanda devlet kontrolündeki bir dijital ortam içinde gözetim, sansür ve siber saldırılar gibi büyük engellerle de karşılaşmaktadır. Yaşanan bu zorluklara rağmen, Suriye'deki siber aktivizm anlatıları şekillendirmede, dayanışmayı güçlendirmede, rejime meydan okumada ve uluslararası alandaki algıları etkilemede önemli bir rol oynamış ve baskıcı ortamlarda siber alanın dönüştürücü potansiyeline dikkat çekmiştir.

Anahtar Kelimeler: Siber Aktivizm, Hacktivist, Suriye, Siber çatışma, Arap Baharı

Introduction

The Syrian conflict, erupting into peaceful demonstrations in March 2011, unveiled a new battleground between the authoritarian regime and activists: the cyber domain. One viral story from the early days of the protests captures the essence of this digital struggle. An intelligence officer, mistakenly searching for a non-existent 'blue device' used by protestors, illustrates the regime's frantic attempts to control and understand the digital tools leveraged by activists.

Under the Baath party's rule since 1963, Syria experienced a stifling environment characterized by restricted freedoms, pervasive fear, and pervasive surveillance. However, the emergence of the Internet in the early 2000s offered Syrians an alternative platform for free expression and dialogue. This digital transformation saw Internet usage surge from a mere 5% in 2005 to approximately 20% by 2012. Cyberspace rapidly evolved into a pivotal arena for activism and resistance against the authoritarian regime. The Syrian Revolution adeptly utilized social media platforms, such as Facebook and Twitter, to document, share, and broadcast the regime's brutal suppression of the protests. Videos, photos, and live streams circulated on these platforms, amplifying the voices of long-suppressed Syrians and drawing international attention to the crisis.

However, the Syrian regime's relationship with cyberspace was complex and multifaceted. Unlike the Egyptian and Libyan regimes, Syria initially lifted blocks on most social media websites and even the emergency law, resulting in a significant surge in social media users. For instance, Facebook users in Syria escalated from a mere 1.5% of the population in early 2011 to 10% by early 2012. While the regime seemingly allowed increased Internet access, it simultaneously cracked down on demonstrations with brutal force, and the absence of foreign news agencies left social media platforms as the primary medium for documenting human rights violations and broadcasting daily events to the global community.

This dynamic transformed cyberspace in Syria into a contested and volatile arena. The regime actively sought to control and monitor the digital landscape by manipulating the infrastructure, installing surveillance systems, imposing restrictive laws, and deploying trained cyber groups to combat cyber activists. Despite these efforts, cyber-activism continued to flourish, illustrating the resilience and adaptability of activists in the face of adversity.

This study aims to delve deeply into the intricate landscape of cyber-activism in Syria, exploring the structure, dynamics, and evolution of online dissent within an oppressive regime. The research seeks to unravel the complexities, constraints, risks, and ethical dilemmas faced by activists in the digital realm. Furthermore, the study will examine the regime's strategies and tools employed to manage and control cyberspace, the activities conducted by activists to overcome these restrictions, and the international community's response to the Syrian cyber crisis.

1. Conceptual Framework: Key Concepts and Debates Related to Cyber-activism

Cyber-activism merges the realms of the "cyber domain" or "cyberspace" with the principles of "activism", leveraging the Internet and communication networks as platforms to advocate for social, political, economic, or environmental change. This modern form of activism utilizes a range of online methods, from social media campaigns to virtual protests, to achieve specific objectives or raise awareness about pressing issues. While cyber-activism

often complements offline activities, it also addresses unique challenges and threats faced in traditional activism, providing an alternative or supplementary avenue for advocacy and mobilization.

The concept of "cyberspace" or "cyber domain" extends beyond technical networks, encompassing the social and contextual effects of the Internet. It represents a symbolic space where all online interactions occur, facilitating a new domain of political interaction and grassroots activism. Questions surrounding user intentions, regulations, and the societal impact of the Internet are actively explored by various stakeholders, including advertisers, businesses, government bodies, and civil society organizations, highlighting the multifaceted nature of the cyber domain.

Distinguishing cyber-activism from other cyber-related terms is crucial for understanding its unique characteristics and objectives. Unlike cyber warfare, which is typically state-initiated and recognized as a form of war, cyber-activism is neither state-led nor internationally recognized as warfare. Additionally, cyber-activism differs from cyberterrorism, which aims to cause destruction or instil fear for ideological purposes. Instead, cyber-activism focuses on instigating socio-political transformation, mobilizing collective voices, and motivating individuals to effect meaningful change through digital means.

1.1. Cyber-Activism, Hacktivism, and Online Engagement

Cyber-Activism and Hacktivism: Cyber-activism, encompassing terms like digital activism and online activism, includes the specific category of hacktivism. Hacktivism involves activists known as Hacktivists who employ cyberattacks, primarily hacking, to advocate for political or human rights causes. The significance of hacktivist cyber-attacks surged notably in 2011 during the Arab Spring, accounting for a substantial portion of recorded cyberattacks.[1] Therefore, hacktivism is considered a subset of cyber-activism, targeting specific causes through cyber means.

Cyber-Activists vs. Cybercriminals and Cyberterrorists: Cyber-activists are distinct from cybercriminals and cyberterrorists in their objectives and methods. While cyber-activists aim to achieve political or societal change through cyber means, cybercriminals target cyber-attacks primarily for financial gain. On the other hand, cyberterrorists engage in operations that can lead to violence or harm. Cyber operations, in this context, refer to strategic activities within cyberspace, such as cyber espionage, hacking, denial of service, and phishing. [2]

Slacktivism or Clicktivism: Not all forms of online engagement qualify as effective cyber-activism. Some activities like sharing or retweeting content require minimal effort and may not yield a significant impact. This superficial form of online participation is termed "slacktivism" or "clicktivism", characterized as "feel-good online activism with zero political or social impact".[3] Examples include liking posts on Facebook, upvoting on Reddit, retweeting on Twitter (referred to as X platform), and changing profile pictures, highlighting the difference between passive online actions and meaningful cyber-activism with tangible societal outcomes.

1 Julie E.Mehan, *Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger*, IT Governance Publishing, United Kingdom, 2015.

2 Johan Sigholm, "Non-State Actors in Cyberspace Operations", *Journal of Military Studies*, 4:1, 2013, pp. 1-37.

3 Tamara Kharroub, "Cyberactivism in the Middle East: Six Potentials and Six Limitations of New Media Technologies in Democratization", *Arab Center Washington DC*, September 2015, https://arabcenterdc.org/resource/cyberactivism-in-the-middle-east-six-potentials-and-six-limitations-of-new-media-technologies-in-democratization, accessed 21.02.2024.

1.2. Characteristics of Cyber-Activism

The advent of the information and telecommunication technology era has dramatically reshaped social and political landscapes, introducing structural opportunities for political participation through almost cost-free access to ICTs. These platforms, particularly social networks, facilitate secure communication among activists, fostering collective identity and virtual communities that mirror real-life interactions.[4] Moreover, the digital realm provides a sanctuary to bypass censorship enforced by authoritarian regimes, allowing for the free exchange and dissemination of information.[5] Anonymity stands as a hallmark of cyber-activism, providing participants with security and enabling them to operate under oppressive regimes. For instance, in Syria, activists utilized pseudonyms on platforms like Facebook to mobilize and inform the public about the oppressive actions of the state, despite decades of restrictions on freedom of assembly and speech.[6]

Inclusive participation is another defining characteristic of cyber-activism, allowing diverse groups to collaborate, voice opinions, and engage in multi-ethnic movements through digital platforms. The Syrian uprising exemplified this inclusivity, with various societal segments, including Arabs, Kurds, youth, and intellectuals, utilizing social media to freely share views and ideas previously suppressed by authoritarian regimes.[7] Furthermore, the digital age has shifted the validation metrics from traditional gatherings to online interactions like likes, retweets, or followers, emphasizing shared validation or dismissal.[8]

Despite its transformative potential, cyber-activism has its limitations. Alone, it may not instigate significant political changes or overthrow regimes, and cyberattacks, a tool of cyber-activism, are not classified as violent attacks under international law due to their non-physical nature.[9] Nevertheless, cyber-activism remains characterized by its accessibility, global reach, anonymity, and ability to break through censorship, providing marginalized groups with a platform to express opinions and oppose ideas without resorting to direct confrontation or violence.

1.3. Types of Cyber Activism

Cyber-activists employ a variety of tactics within the digital realm to advocate for causes, resist oppression, and mobilize public opinion. These activities are often tailored to the nature of the proposed action, the tools at their disposal, and the specific objectives they aim to achieve. A primary form of cyber-activism is Citizen Journalism, where activists leverage platforms like blogs, Facebook, Twitter, and YouTube to highlight government abuses, advocate for political change, and influence public opinion. Social media enables instant news dissemination, live-streaming of protests, and rallying citizens to resist oppressive regimes.[10]

4 Courtney Radsch, *Cyberactivism and Citizen Journalism in Egypt: Digital Dissidence and Political Change*, Palgrave Macmillan, New York, 2016.

5 Yenal Göksun, "Cyberactivism in Syria's War: How Syrian Bloggers Use Internet for Political Activism", BAYBARS-HAWKS Banu (eds.), *New Media Politics: Rethinking Activism and National Security in Cyberspace*, Cambridge Scholars Publishing, 2015, pp. 49-62.

6 Scott Applegate, "Cyber-militias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security & Privacy*, 9:5, 2011, pp. 16-22.

7 Sahar Khamis, Paul Gold, and Katherine Vaughn, "Beyond Egypt's 'Facebook Revolution' and Syria's 'Youtube Uprising:' Comparing Political Contexts, Actors and Communication Strategies.", *Arab Media & Society*, 15:1, 2012, pp.1-30.

8 Courtney Radsch, *Cyberactivism and Citizen Journalism in Egypt: Digital Dissidence and Political Change*, Palgrave Macmillan, New York, 2016.

9 Scott Applegate, "Cyber-militias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security & Privacy*, 9:5, 2011, pp. 16-22.

10 Sahar Khamis, Paul Gold, and Katherine Vaughn, "Beyond Egypt's 'Facebook Revolution' and Syria's 'Youtube Uprising:' Comparing Political Contexts, Actors and Communication Strategies.", *Arab Media & Society*, 15:1,

Another prevalent category is Online Petitions, Demonstrations, and Campaigns, where the Internet serves as a platform for raising funds, creating international alliances, and coordinating events. This digital space becomes crucial in shaping public opinion, with contrasting narratives vying for attention and aiming to influence specific audiences.[11] Digital Literacy and Cybersecurity Safety Training also play a vital role in cyber-activism. Training activists in digital literacy equips them with essential skills to protect themselves online, especially in regimes with strict censorship or limited technical expertise.

Cyber-attacks form another facet of cyber-activism, often carried out by hacktivists targeting government, corporate, or politically aligned entities. These attacks aim to exert influence, cause damage, or infiltrate opposition communication systems, with motives ranging from expressing disapproval to raising public awareness.[12]

While these categories provide a broad overview, cyber-activism can be further segmented based on objectives, as Sander Vegh suggests, into Awareness/Advocacy, Organization/Mobilization, and Action/Reaction. Awareness/Advocacy involves disseminating information online through various channels like email lists and social media networks. Organization/Mobilization leverages online platforms to call for offline or online actions, such as protests or global pressure campaigns. Lastly, Action/Reaction encompasses hacktivist-led cyber-attacks, targeting specific online entities through techniques like denial-of-service attacks or website hijacking to gain critical information.[13]

1.4. Tools Of Cyber-Activism

Social Media Networks and Blogging: The digital landscape has provided a plethora of tools for cyber-activists, with social media platforms and blogging standing out as prominent mediums for mobilization and awareness-raising. Facebook serves as a pivotal platform for communication and mobilization, facilitating connections among like-minded individuals and rallying support around specific causes. Notably, the "We are all Khaled Said" Facebook page played a significant role in galvanizing public sentiment against human rights violations in Egypt, ultimately catalysing the 2011 revolution.[14] Twitter, on the other hand, excels in real-time organization and coordination, as evidenced by its instrumental role during the Tahrir Square protests in Egypt.[15] The platform's allowance for pseudonyms also makes it an attractive option for activists prioritizing anonymity. In response to Facebook's stricter policies and account deletions, many cyber-activists have turned to blogging as an avenue for unrestricted self-expression, shedding light on taboo subjects and facilitating public discourse on issues like government corruption and human rights violations.[16] Moreover, the use of hashtag in social media has been considered as a form of digital activism by employing hashtags on social media networks. Although research on hashtag activism is still considered relatively new, many hashtag campaigns have gained attention as a popular strategy for

2012, pp.1-30.

11 Martha McCaughey and Michael D. Ayers, *Cyberactivism: Online Activism in Theory and Practice,* Routledge, New York, 2003.

12 Ibid.

13 Ibid.

14 Sahar Khamis and Katherin Vaughn, "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,* 4:2-3, 2012, pp. 145-163.

15 Courtney Radsch, *Cyberactivism and Citizen Journalism in Egypt: Digital Dissidence and Political Change*, Palgrave Macmillan, New York, 2016.

16 Sahar Khamis, "Revisiting Cyberactivism Six Years After the Arab Spring: Potentials, Limitations and Future Prospects", Nele Lenze, Charlotte Schriwer & Zubaidah Abdul Jalil (eds), Media in the Middle East, Palgrave Macmillan Cham, 2017, pp. 3-19.

driving socio-political changes worldwide through social media.[17] Twitter hashtags, for example, have been crucial in developing counter-narratives, mobilizing supporters, and creating diverse support networks. The #BlackLivesMatter movement spread rapidly after the murder of Trayvon Martin, a black teenager in the United States, in 2012.[18]

Cyber-Attack Tools: While cyber-activists leverage digital tools for advocacy and mobilization, they also face adversaries wielding similar tools for malicious purposes. Hacktivists often employ 'Advanced Persistent Threats' (APTs) for information exfiltration and cyber espionage, infiltrating systems clandestinely to gather data over extended periods without detection. Distributed Denial of Service (DDoS) attacks represent another prevalent method used by malicious actors to disrupt online services by inundating them with excessive traffic.[19] Malware attacks, including viruses, worms, and Trojans, pose significant threats as well, with the FinFisher spyware application being used by Egyptian authorities to monitor dissidents during the Egyptian Revolution.[20] Phishing scams further compound the risks, with perpetrators exploiting deception to trick individuals into divulging sensitive information. These cyber-attack methods have been employed extensively during events like the Syrian uprising, targeting both hacktivist groups and government-allied non-state actors.[21]

Internet Access and Safety Tools: In the face of government-imposed Internet shutdowns and extensive censorship, cyber-activists have had to innovate and adapt to maintain communication channels and access vital information. In regions like Syria, where complete Internet blackouts have been enforced in conflict zones, activists have resorted to alternative means of Internet access, including smuggling communication equipment and utilizing SIM cards from neighbouring countries. To circumvent website blocks and ensure secure communication, cyber-activists employ Anonymous Browsing Tools like TOR and Virtual Private Networks (VPNs). TOR routes Internet traffic through a global server network, preserving users' anonymity and location, while VPNs encrypt Internet connections, offering crucial protection against surveillance and enabling access to blocked websites and social media platforms.

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

Cyber-activism harnesses the power of the Internet and digital platforms to empower individuals, particularly in authoritarian regimes, where traditional political participation is constrained by fear of persecution.[22] Social media and Web 2.0 technologies offer a safe and cost-effective means for ordinary people, including minority groups, to voice their opinions, organize collective actions, and mobilize global public support.[23] In countries like Syria,

17 Manash Goswami, "Social Media and Hashtag Activism", *Liberty Dignity and Change in Journalism*. Kanishka Publisher, New Delhi, 2018, pp. 252-262.

18 Burak İli, "Bibliometric Analysis of Hashtag Activism Researches", *Turkish Online Journal of Design, Art and Communication*, 13:4, 2023, pp. 900-915.

19 Julie E.Mehan, *Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger*, IT Governance Publishing, United Kingdom, 2015.

20 John Leyden, "UK Firm Denies Supplying Spyware to Mubarak's Secret Police", The Register, 21 September, 2011, https://www.theregister.com/2011/09/21/gamma_international_denies_egyptian_links, accessed 20.2.2024.

21 Nino Guruli And Sarah Dávila-Ruhaak. "Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023.

22 Masudul Biswas and Carrie Sipes. "Social Media in Syria's Uprising and Post-Revolution Libya: An Analysis of Activists' and Bloggers' Online Engagement", *Arab Media & Society*, Fall 2014 (19):1, 2014, pp. 1-21.

23 Scott Applegate, "Cyber-militias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security & Privacy*, 9:5, 2011, pp. 16-22.

where physical dissent is restricted, the Internet plays a crucial role in communication and information sharing, enabling real-time access to ground events and exposing state brutality.[24]

Cyber-activism operates on two fronts: leveraging cyberspace to address offline issues by shaping public opinion, mobilizing masses, achieving political objectives, and operating within the digital domain to ensure the free flow of information and safeguard citizens' interests.[25] Thus, cyber-activism has evolved into a movement deeply rooted in cyberspace, striving to promote socio-political transformation and uphold democratic values.

In countries like Syria, where physical gatherings and open dissent are severely restricted under repressive regimes, the Internet has become an indispensable tool for communication and information sharing. A Syrian human rights activist emphasized the importance of the Internet, stating, "The Internet is the only option for intellectuals to meet and share ideas".[26] Cyberspace and social media networks played a pivotal role in preventing the immediate suppression of the revolution in Syria.[27] The widespread access to mobile information technologies and high levels of e-literacy among citizens enabled unprecedented real-time access to ground events. This facilitated the dissemination of critical information, including images of casualties and statements highlighting violent acts, thereby exposing the severity of state brutality.[28]

1.6. Limitations of Cyber-Activism

Despite its potential, cyber-activism faces significant challenges. Overcoming these obstacles is crucial to ensuring its effectiveness and inclusivity as a platform for civic engagement and social change.

- Internet Access and Digital Divide: Cyber-activism is limited by unequal Internet access and digital literacy, especially in less-developed regions. For example, in Syria, only 22% of the population had Internet access in 2014.[29]
- Internet Surveillance and Government Control: Government surveillance and online censorship restrict online freedoms, particularly in authoritarian regimes. In Syria, strict regulations require citizens to obtain government approval for Internet devices, and major social media platforms aid in monitoring activists.[30]
- Limitations of Social Media Platforms: social media can create echo chambers, fostering polarization and hindering balanced discussions. They can catalyse change, as seen in the Egyptian Revolution, but also exacerbate divisions

24 Shawn Powers and Ben O'Loughlin, "The Syrian Data Glut: Rethinking the Role of Information in Conflict", *Media, War & Conflict,* 8:2, 2015, pp 172-180.

25 Chang Woo-Young and Lee Won-Taek, "Cyberactivism and Political Empowerment in Civil Society: A Comparative Analysis of Korean Cases", *Korea Journal*, 46:4, 2006, pp. 136-167.

26 Tamara Kharroub, "Cyberactivism in the Middle East: Six Potentials and Six Limitations of New Media Technologies in Democratization", *Arab Center Washington DC*, September 2015, https://arabcenterdc.org/resource/cyberactivism-in-the-middle-east-six-potentials-and-six-limitations-of-new-media-technologies-in-democratization, accessed 21.02.2024.

27 Masudul Biswas and Carrie Sipes. "Social Media in Syria's Uprising and Post-Revolution Libya: An Analysis of Activists' and Bloggers' Online Engagement", *Arab Media & Society*, 19:1, 2014, pp. 1-21.

28 Shawn Powers and Ben O'Loughlin, "The Syrian Data Glut: Rethinking the Role of Information in Conflict", *Media, War & Conflict,* 8:2, 2015, pp. 172-180.

29 Yenal Göksun, "Cyberactivism in Syria's War: How Syrian Bloggers Use Internet for Political Activism", BAYBARS-HAWKS Banu (eds), *New Media Politics: Rethinking Activism and National Security in Cyberspace*, Cambridge Scholars Publishing, 2015, pp. 49-62.

30 Faten A. Mansour, "Cyber-Activism: Engendering Political Subjects Within New Logics of Resistance in Contemporary Egypt and Yemen", Master's thesis, The American University in Cairo, Cairo, Egypt, 2016.

post-movement. Algorithmic censorship and platform decentralization further complicate matters.[31]

- Challenges of Citizen Journalism: Citizen journalism, while offering grassroots perspectives, lacks professional rigour and is susceptible to misinformation and inaccuracies.[32]
- Limited Impact of Cyber-Attacks in Undeveloped Countries: In regions with limited ICT infrastructure, like Syria, cyber-attacks have minimal impact on achieving cyber-activism goals due to the absence of e-government and robust digital platforms.

2. Methodology

The study focuses on the rise of cyber-activism in Syria, exploring its opportunities and limitations. It examines how cyberspace's structure impacts cyber-activism's efficacy and the interplay between cyber and on-ground conflicts, specifically how activists influence authoritarian regimes.

The study aims to distinguish cyber-activism from cyber warfare, examining its potential and limitations during various conflict phases. It seeks to build knowledge on using cyber-activism for political change. Additionally, it investigates how the Syrian regime's cyber-surveillance system impacts the efficiency of cyber-activism. The central question of this study is how cyber-activism can be understood within the context of the authoritarian regime in Syria.

To answer this question, the research employs qualitative methodologies, including theoretical studies to provide a foundational understanding of cyber-activism, academic research on global cyber-activism and regional studies, official reports from reputable organizations and case studies and semi-structured interviews with nine Syrian cyber-activists and cyber experts were working in the cyber domain management in Syria. Two different semi-structured interview questions were used during the interviews, one for cyber experts and the other for cyber activists. The interviews were structured around ten questions covering the interviewee's role, the challenges they faced, and the reactions from authorities.

The study covers the period of 2007-2016, capturing the peak of online activism and the Syrian regime's surveillance developments. Due to security reasons, the study does not include state-backed cyber-activists or intelligence forces but compensates by referencing existing studies on the topic. Transcriptions were analysed to identify recurring themes and patterns. Pseudonyms were used for all interviewees to protect their identities.

The interviewees' profiles with their pseudonyms, as well as their role during the cyber-activism in Syria, are explained as the following:

- 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.

31 Sahar Khamis, "Revisiting Cyberactivism Six Years After the Arab Spring: Potentials, Limitations and Future Prospects", Nele Lenze, Charlotte Schriwer & Zubaidah Abdul Jalil (eds.), *Media in the Middle East*, Palgrave Macmillan Cham, 2017, pp. 3-19.
32 Ibid.

- Samer, a 44-year-old activist and ICT expert, lived outside Syria when the revolution started and supported activists via satellite Internet before returning to Syria. He spent a long period in a besieged region.
- Wafi, 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 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. Yusuf 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. Kareem was responsible for applications that monitor the network.

3. Cyberspace Landscape in Syria

The evolution of global telecommunications technology has transformed the role of media, expanding from basic news transmission to shaping public opinion and disseminating cultural values. The advent of the Internet revolutionized information dissemination, with Internet users surpassing radio users in just a fraction of the time it took for radio to reach the same milestone. In Syria, however, Internet access was restricted until 1999, with citizens initially barred from subscribing. The government's cautious approach towards Internet access reflected its efforts to control expression critical of its governance, viewing the Internet as a potential threat to its authority. Nonetheless, some state institutions have had limited Internet access since 1997, hinting at a gradual shift in the regime's stance towards online connectivity.

3.1. Cyberspace in Syria: Historical Context and Infrastructure

The Ba'ath Party, in power since 1963, imposed emergency law, granting the state sweeping control over communication and media institutions, severely restricting individual liberties. The media served as a tool for reinforcing dictatorship, disseminating the ruling party's message, and projecting the image of the president, Hafez al-Assad. Despite the Arab world's media transformation in the 1990s, Syria lagged in granting Internet access, initiating a cautious trial project in 1996, which officially began in 1997, initially catering to a limited

number of subscribers from government entities.[33] Bashar al-Assad's ascension to power in 2000 brought promises of expanded Internet access, with subscription approval often contingent on security clearance, reflecting the regime's security-centric approach. Internet penetration gradually increased from 0.2% in 2000 to around 35% in 2021, indicating a significant but controlled expansion of online connectivity in Syria.[34]

3.2. Governmental Entities and Corporate Bodies

Cyberspace in Syria is heavily regulated and controlled by the government through various ministries and entities. The following are the governmental bodies and entities involved in managing the cyber domain in Syria.

- **Ministry of Communications and Technology (MoCT):** MoCT oversees national policies and strategies related to information, communications, and postal sectors. It promotes technology's role in economic and social development.[35]
- **Syrian Telecommunications Establishment (STE):** Established in 1975, STE is pivotal in Syria's cyber domain, providing global connectivity and regulating information flow. It has alliances with foreign companies and collaborations with local mobile service providers.[36]
- **National Agency for Network Services (NANS):** Established in 2009, NANS regulates electronic transactions and enhances network service efficiency, enforcing security measures.[37]
- **Syrian Telecommunication Regulatory Authority (SyTRA):** SyTRA regulates the telecommunications sector, ensuring service quality, fostering competition, and representing Syria in global communication forums.[38]
- **Syrian Computer Society (SCS):** The Syrian Computer Society (SCS), founded in 1989 by Bassel Assad, aims to promote and advance Information Technology (IT) and Computer Science in Syria. Despite being an independent civil organization, the SCS has maintained strong ties with the government and has played a crucial role in the development of IT in the country. After Bassel Assad's sudden death in 1994, Bashar Assad took over the leadership of the SCS until his presidency in 2000. The SCS organizes various training sessions, meetings, and conferences to enhance computer literacy and has established its own Internet services provider, SCS-NET, contributing significantly to the expansion of IT infrastructure and services across Syria.[39]
- **Syriatel:** Established in 2000, Syriatel is the primary mobile service provider in Syria's growing telecommunication market. By 2014, the company had expanded

33 "Syrian Center for Media and Freedom of Expression". Internet Media, https://scm.bz/en, accessed 5.3.2024.

34 Nino Guruli And Sarah Dávila-Ruhaak. "Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023.

35 "Ministry of Communication and Technology". https://shorturl.at/5yRih, accessed 14.3.2024.

36 Julie Racicot, The Syrian Civil Conflict in the Cyber Environment, Master's thesis, Royal Military College of Canada, Kingston, Canada, 2015.

37 "National Agency for Network Services", https://nans.gov.sy/ar/page/establishment_of_the_national_network_se, accessed 22.03.2024.

38 "Syrian Telecommunication Regulatory Authority", https://www.sytra.gov.sy/index.php/en/about-us, accessed 5.2.2024.

39 Julie Racicot, The Syrian Civil Conflict in the Cyber Environment, Master's thesis, Royal Military College of Canada, Kingston, Canada, 2015.

its network across the country and amassed a customer base of seven million, competing primarily with MTN as its only competitor. Additionally, SyriaTel owns SAWA, one of Syria's largest Internet Service Providers (ISPs). Despite facing American sanctions since April 2012, the company has continued to establish partnerships with Chinese firms. Like other service providers in Syria, SyriaTel's traffic is routed through the Syrian Telecommunications Establishment (STE). Initially owned by Rami Makhlouf, a cousin of President Bashar Assad, who also served as its CEO, the Syrian government ordered the confiscation of Makhlouf's assets in mid-2020.[40]

- **MTN:** It is Syriatel's only competitor. 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.[41]
- **Private Internet Service Providers:** Since 2005, private ISPs have increased, with an estimated 14 operating today. However, all connections must pass through STE and comply with NANS policies.

3.3. The Role of the Syrian Government in Controlling and Monitoring Cyberspace

The Syrian government exerts stringent control and monitoring over the cyber domain despite the substantial growth in Internet usage since 2005. Initially, the Syrian Telecommunications Establishment (STE) limited Internet access to a minimal number of subscribers, which increased to approximately 4 million by 2010. Despite this apparent openness, the government imposed numerous restrictions on Internet use, requiring all Internet Service Providers (ISPs) to monitor user activities and mandating Internet café owners to record customer details and online activities.[42]

Documents obtained by Privacy International reveal that STE employs advanced Western technology to intercept real-time communications, including phone calls, text messages, emails, and VoIP services. STE's focus on addressing 'propaganda mail' suggests an intent to counter specific cyber-activism tools.[43] The STE launched Syria's first nationwide surveillance system in 1999 and invited bids in 2007 to develop a centralized Internet monitoring system capable of content filtering, data analysis, and real-time tracking of individuals without their knowledge.[44]

Furthermore, reports from Citizen Lab at the University of Toronto indicate that the Syrian government utilizes telecommunication monitoring devices from Blue Coat Systems, a U.S.-based company, for network filtering, censorship, and surveillance. Despite U.S. sanctions prohibiting sales to Syria, these devices were reportedly shipped to a distributor in

40 "Syrian Government Orders Seizure of Assets of Rami Makhlouf", *Al-Jazeera*, May 19, 2020. https://www.aljazeera.com/economy/2020/5/19/syrian-government-orders-seizure-of-assets-of-rami-makhlouf, accessed 12.03.2024.

41 "MTN Syria", https://en.wikipedia.org/wiki/MTN_Syria, accessed 12.3.2024.

42 Rey Matthieu "Preventing a Mobilization from Spreading: Assad and the Electronic War", Nele Lenze, Charlotte Schriwer & Zubaidah Abdul Jalil (eds), *Media in the Middle East*, 2017, Palgrave Macmillan Cham, 2017, pp. 89-106.

43 "Open Season: Building Syria's Surveillance State", Privacy International, December 2016, http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state, accessed 20.11.2023.

44 Ibid.

Dubai and subsequently deployed in Syria.[45] These devices employ deep packet inspection (DPI) to analyse data packets, allowing detailed content examination.

Interviews with cyber experts corroborate the government's control over the cyber domain. Kareem, a former employee of the Syria Computer Society (SCS), revealed that the SCS initially had a direct marine connection to the global network through Cyprus. However, the government restricted access to the global network exclusively through STE. Despite being major telecommunications companies, Syriatel and MTN have limited control over Internet services. Syriatel relies entirely on STE for Internet connectivity and is subject to the Syrian Telecommunication Regulatory Authority's (SyTRA) pricing regulations. Both companies are obligated to maintain copies of all calls and messages and provide STE with necessary equipment and server access. MTN, being an international company, has servers located within STE buildings, with stringent security measures in place.

3.4. Intelligence Forces Power in Cyberspace in Syria

In Syria, often referred to as the "Kingdom of Silence", the authoritarian regime exercises pervasive control over all aspects of life through an extensive intelligence apparatus comprising four central bodies, two divisions, and two directorates. These intelligence entities, which include Military Intelligence, Air Force Intelligence, Political Intelligence Department, and General Intelligence Department, are affiliated with either the Ministry of Defence or the Ministry of Interior. Each division and department operates numerous central and regional branches across the country, responsible for monitoring various aspects ranging from military and police forces to civil activists.[46] The regime requires approvals from these security authorities for any collective activities, including religious events, humanitarian actions, and even weddings.

Given the rise of the cyber domain as a platform for gathering, sharing, and disseminating information, specialized intelligence branches have been established to monitor this digital space. These branches are primarily affiliated with the Military Intelligence Division and include:

- **Branch 225**: known as the Communication Branch, exercises dominant control over all communication-related activities within Syria. It has the capability to block specific numbers, terminate calls, disable SMS services, intercept messages, and monitor phone calls. As the Syrian revolution unfolded, this branch assumed comprehensive management of the cyber domain, with personnel sourced from various other branches and departments.[47]
- **Branch 211:** referred to as the "Technical" or "Computer" branch, focuses on Internet-related affairs, regulating website access, managing wireless communications, and providing technical support to Branch 225.[48]

45 "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools", Citizen Lab, 15 January 2013, https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/, accessed 12.02.2024.

46 Nino Guruli And Sarah Dávila-Ruhaak. "Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023.

47 "Branch 215, Raid Brigade Military Intelligence Division", *Violations Documentation Center*, 2013, http://t.co/t53aZ4XbJb, accessed 3.10.2023.

48 Maen Tallaa, "The Syrian Security Services and the Need for Structural and Functional Change", Omran for Strategic Studies, 18 November 2016, https://omranstudies.org/index.php/publications/papers/the-syrian-security-services-and-the-need-for-structural-and-functional-change.html, accessed 21.10.2023.

- **Branch 237**: specializes in tracking and tapping wireless calls, with expertise in scanning wireless and radio waves.[49]
- **Digital Security Branch:** established in 2019 with Russian support, operates under the Department of Political Intelligence and specializes in cyber and information security, directly supervised by Russian officers.[50]

These specialized branches, equipped with surveillance equipment and devices maintained by the Syrian Telecommunications Establishment (STE), enable the intelligence apparatus to exert broad monitoring and control over the cyber domain, allowing comprehensive surveillance of all activities.[51]

3.5. International Presence in Syrian Cyber-space

The Syrian Telecom Establishment (STE) has engaged with international ICT companies to facilitate censorship and surveillance despite sanctions. 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):** Blue Coat's devices were found active in Syria, violating U.S. sanctions. The company denies direct sales but acknowledges its devices' presence in Syria.[52]
- **Advanced German Technology AGT (Germany):** AGT provides censorship solutions in Syria through its Dubai operation, bypassing U.S. sanctions.[53]
- **RCS S.p.A (Italy):** In collaboration with AGT, RCS offers centralized monitoring systems in Syria.
- **VASTech (South Africa):** VASTech, in partnership with AGT, has supplied censorship solutions in Syria since 2002.
- **Amesys (France):** Amesys, while denying direct contracts with Syria, acknowledges AGT as its Middle East distributor.
- **Utimaco (Germany):** Utimaco provided an interception system to Siemens for Syria in 2004, allowing real-time communication interception.
- **AREA (Italy):** AREA won a bid for STE's monitoring system but withdrew after U.S. export regulation violations.[54]
- **Qosmos (French):** Qosmos supplied the STE with Deep Packet Inspection tools, terminating the project in 2012.[55]

49 "Syrian Security Branches and Persons in Charge*"*. Syrian Network for Human Rights, https://snhr.org/public_html/wp-content/pdf/english/Syrian_security_branches_and_Persons_in_charge_en.pdf, accessed 5.01.2024.
50 "Russia Restructures Military Intelligence Network to Disrupt Support for Ukraine", Asharq Al-Awsat, 2024, https://shorturl.at/CglBH, accessed 24.2.2024.
51 Julie Racicot, The Syrian Civil Conflict in the Cyber Environment, Master's thesis, Royal Military College of Canada, Kingston, Canada, 2015.
52 Morgan Marquis-Boire, Jakub Dalek et al., "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*"*, Citizen Lab, 15 January 2013 ,https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/, accessed 12.02.2024.
53 "Open Season: Building Syria's Surveillance State", Privacy International, December 2016, http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state, accessed 20.11.2023.
54 Ibid.
55 Kitetoa Antoine Champagne, "Network Surveillance: Qosmos, a Tool Provider for Syria's Leader Al-Assad",

- **Huawei (China):** By 2009, Syriatel had shifted to Huawei's infrastructure, assisting in telecommunication censorship.

In essence, international firms have significantly contributed to Syria's cyber-surveillance capabilities, often sidestepping sanctions and regulations.[56]

3.6. Cyberspace as a Tool of Repression in Syria

The Syrian regime has constructed a sophisticated surveillance infrastructure since allowing Internet access in the country. The Syrian Telecom Establishment (STE) was designated the sole gateway to the global Internet, with all ISPs and telecom companies mandated to adhere to its regulations. Various intelligence branches, notably Branch 225, monitor and track online communications, exposing cyber-activists to privacy breaches and potential targeting.[57]

Privacy International outlined key strategies employed by the Syrian regime for online surveillance and censorship by centralizing Internet connectivity through STE, directing all national Internet traffic via STE servers, and using STE as a cover for intelligence operations, particularly by Branch 225.[58]

Research from the Syrian Center of Media and Freedom of Expression highlighted a shift in censorship strategies over time:

- 1999-2005: A restrictive approach blocking most services, including email and FTP.
- Post-2005: A more lenient policy allowing most services but selectively blocking certain websites, overseen by STE in collaboration with intelligence agencies.[59]

Moreover, in 2012, the Syrian government introduced the Informatics Crime Law, which was subsequently amended several times. This legislation mandates website owners to archive content and traffic data. Also, it requires disclosure of contributor identities to the government and criminalizes the dissemination of false news detrimental to the state, putting activists and journalists at risk.[60]

Consequently, this surveillance often leads to arrests, torture, and even fatalities, as reports from Citizen Lab and insider accounts, such as Fredric Jacobs, have detailed the Syrian regime's use of digital surveillance to monitor activists.[61]

3.7. Incidents Illustrating Government Control Over Online Activities in Syria

While Syria appeared to have relaxed its online censorship around 2005, several incidents reveal the government's control over online activities:

Reflets, 09 May 2014, https://reflets.info/articles/network-surveillance-qosmos-a-tool-provider-for-syria-s-leader-al-assad, accessed 13.1.2024.

56 "Open Season: Building Syria's Surveillance State", Privacy International, December 2016, http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state, accessed 20.11.2023.

57 Walid Al-Saqaf, "Internet Censorship Circumvention Tools: Escaping the Control of the Syrian Regime", *Media and Communication,* 4:1, 2016, pp. 39-50.

58 "Open Season: Building Syria's Surveillance State", Privacy International, December 2016, http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state, accessed 20.11.2023.

59 "Syrian Center for Media and Freedom of Expression". Internet Media, https://scm.bz/en, accessed 5.3.2024.

60 "Ministry of Communication and Technology". https://shorturl.at/5yRih, accessed 14.3.2024.

61 Nino Guruli And Sarah Dávila-Ruhaak. "Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023.

- Muhammad Ghanem: Founder of the Souryoun website, arrested on 31 March 2006 and sentenced to six months in prison for publishing media materials deemed insulting to the state and inciting sectarian strife.[62]
- Tal Al-Mallouhi: "The youngest Internet Prisoner", Al-Mallouhi was arrested on 27 December 2009 by State Security forces. She was known for her political and social blogs and was eventually sentenced to five years in prison in February 2011. Her case gained international attention and sparked protests demanding her release.[63]
- Akram Raslan: A cartoonist arrested for drawings deemed offensive to the state's prestige. Raslan disappeared after his detention and was reported to have died from torture in 2013.[64]

Ziad, who was working in the Syriatel headquarters office, disclosed the extensive surveillance capabilities of the government:

- Mobile Switch Centre (MSC): Capable of tracking the location of even switched-off devices.
- Call Tracking: Specific call information can be retrieved upon request, primarily from Intelligence Branch 225 and occasionally from STE.

Ziad recounted an incident where a list of over 10,000 contact numbers for tracking was leaked from Syriatel and which resulted in a thorough investigation inside the company. Furthermore, he also mentioned an instance where the president's cousin used his influence to track his girlfriend's movements covertly through STE by Syriatel location tracking capabilities.

3.8. Surveillance System and Censorship

Syria has deployed a range of surveillance measures to monitor and control digital communications. According to interviews, Syriatel, the country's leading telecom provider, implemented SMS filters targeting messages containing location, time, and date information to obstruct protest coordination. The Syrian Telecommunications Establishment (STE) has also mandated the blocking of unauthorized SMS broadcasting, restricting this service to companies registered with STE. Furthermore, all digital communications, including calls, SMS, and MMS, are systematically recorded, with intelligence agencies having direct access to this data.

On the other hand, the Syrian government has adopted a nuanced approach to online censorship over the years. Between 1999 and 2005, Syria enforced stringent restrictions on Internet services, including the blocking of websites containing the word "Mail" and hindering FTP and popular email platforms.[65] Although the censorship policy shifted in 2005 to "allow everything, block some services", major social media platforms like Blogger, Facebook, YouTube, and Twitter remained inaccessible until 2011. To enforce these censorship measures, Syria employed Blue Coat servers to filter websites and block contents.

62 "Syrian Center for Media and Freedom of Expression". Internet Media, https://scm.bz/en, accessed 5.3.2024.
63 "Syria: Tal al-Mallohi sentenced after flawed trial", Amnesty International, 18 February 2011. https://www.amnesty.org/fr/wp-content/uploads/2021/07/mde240062011en.pdf, accessed 24.1.2024.
64 Nino Guruli And Sarah Dávila-Ruhaak. "Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023.
65 "Syrian Center for Media and Freedom of Expression". Internet Media, https://scm.bz/en, accessed 5.3.2024.

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 to monitor communications in real-time. 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, including FTP and popular email services, were blocked. 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.

4. The Rise of Cyberconflict in Syria

With the emergence of protests in Syria in March 2011, cyberspace emerged as the only safe haven for activists, given that physical gathering spots were heavily monitored. Activists utilized the digital realm for organizing, idea-sharing, mobilizing, and coordinating protest activities. Social media platforms became instrumental in the dissemination of news about the violent crackdown on protestors, filling the void left by the absence of independent news channels and international press. Amjad Baiazy, a Syrian activist, shared the transformative role of cyberspace in Syrian activism: "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... Now we are a group of twenty-five media activists in my town".[66]

4.1. Cyber Domain: A Mobilizing and Coordination Space

While social media platforms like Facebook, YouTube, Twitter, and blogging sites had been blocked since 2007 due to government censorship, the Syrian regime surprisingly unblocked Facebook and YouTube in February 2011. This decision came shortly after the successful use of social media in Egypt to mobilize anti-government protests. While this allowed activists to better coordinate and mobilize, it also exposed them to detection by the government. Racicot highlighted the rapid rise in Syrian Facebook accounts after the unblocking: "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".[67] Ahmad, a cyber-activist, detailed his journey from a casual social media user to an activist leveraging these platforms for coordination, sharing, and organizing protests under "coordination units". These units operated under pseudonyms to protect their identities and employed a network of trust to ensure security. Abdulkadir, an activist in Damascus, mentioned how they used Facebook under fake names to coordinate protests, eventually building a network of 150 people. Ahmad noted his shift from Facebook to Twitter for broader reach, especially outside Syria, while also highlighting the shift in content from long articles to quick updates and breaking news.

66 Amjad Baiazy, "*Syria's Cyber War"*, https://www.academia.edu/3555530/Syria_Cyber_Wars, accessed 3.2.2024.
67 Julie Racicot, The Syrian Civil Conflict in the Cyber Environment, Master's thesis, Royal Military College of Canada, Kingston, Canada, 2015.

Samer, a computer engineer and cyber-activist living abroad during the onset of the Syrian protests, highlighted the development of an interactive map showing protest locations and participant numbers. This map served as a foundation for a cyber-activist group that started live video streaming to counter the absence of news agencies and media networks. "We were a team of no more than 15 people... 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", Samer said.

4.2. Authoritarian Countermeasures: Intelligence Forces Response

Rey Matthieu's study revealed that the Syrian regime effectively used cyberspace as a tool for intelligence, enabling them to track and arrest activists. When activists were arrested, they were often subjected to physical torture to extract social media credentials. This led to increased distrust within activist circles. To counteract this, expert cyber-activists from the group "Anonymous" stepped in to assist by implementing advanced secure browsing tools like Tor and training activists on using VPNs for enhanced protection.[68]

Racicot detailed other authoritarian countermeasures, such as slowing down Internet speeds on Fridays, known protest days, to hinder the uploading of videos and photos and real-time traffic monitoring. Additionally, complete Internet shutdowns were reported in regions experiencing massive protests or military operations. Branch 225 ordered mobile operators like MTN and Syriatel to filter and block SMS messages containing words indicative of protest coordination or participation. Ahmad recounted how simple text messages indicating protest times or locations began failing to send over the network, signalling an intensified crackdown on digital activism.[69]

4.3. Overcoming the Digital Curtain and Defying Digital Oppression

Cyber-activists in Syria circumvented Internet blackouts and bandwidth restrictions by using satellite Internet and neighbouring countries' Internet connections. These methods allowed high-speed Internet access and bypassed censorship mechanisms imposed by STE, which became essential, especially after the regime cut off communications in certain areas.

On the other hand, cyber-activists sought alternatives to local Internet due to surveillance and periodic shutdowns by the Syrian regime. Some activists were arrested due to using Thuraya satellite solutions, leading to mistrust in the company. They shifted to European-based companies like Inmarsat, Astra, and tooWay, believing satellite Internet could evade surveillance. However, concerns arose over the collaboration between the United Arab Emirates (UAE) and the regime, leading to targeted assassinations based on device coordinates.

Furthermore, activists employed measures like using pseudonyms, VPNs, and protective software to conceal their identities and activities. There was a collective effort to share knowledge and resources on cybersecurity. While social media presented challenges for regime control, arbitrary arrests at military checkpoints increased, highlighting the regime's need for social media literacy. Activists used dual social media accounts, one for checkpoints and another for activism, to minimize risks.

68 Rey Matthieu "Preventing a Mobilization from Spreading: Assad and the Electronic War", Nele Lenze, Charlotte Schriwer & Zubaidah Abdul Jalil (eds.), *Media in the Middle East*, 2017, Palgrave Macmillan Cham, 2017, pp. 89-106.

69 Nino Guruli And Sarah Dávila-Ruhaak. "Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023.

4.4. Intervention of the Intelligence Branches and Digital Detention

Syrian intelligence branches have extensive monitoring capabilities in the cyber domain, accessing surveillance equipment and monitoring activities inside telecommunication companies. Syriatel, a major telecommunication company, transformed into an intelligence branch with increased surveillance and security measures. Employees faced arrests and investigations due to information leaks. Meanwhile, another telecom company, MTN, operated differently and was seemingly treated as an international entity.

As a result, cyber-activists faced arrests, with some detained for mere social media activity like "liking" certain pages. The intelligence services used detainees' social media accounts to track and entrap others, leading activists to close accounts remotely when someone was arrested. The regime appeared to target tech-savvy individuals, making them vulnerable due to their contributions to digital communication infrastructure. The narratives reflect the challenges faced by Syrian cyber-activists in maintaining digital freedoms and the lengths to which they went to resist digital oppression and surveillance by the regime.

4.5. Limited International Support for Cyber-Activists

Despite the critical role played by cyber-activists in Syria's civil unrest, there appears to be limited international support for their efforts, particularly in terms of training and resources for cyber-attacks. Barrow highlighted that while civilian journalists received training on navigating Internet censorship and securely sending media materials, this support seems insufficient in the broader context of cyber-activism.[70]

Multinational hacktivist groups like Anonymous, known for their cyber-attacks on various entities, operated on a voluntary and unorganized basis. There is no evidence to suggest that these groups received any formal backing from countries, organizations, or governmental entities. Furthermore, cyber-activists often had to bear the financial burden of their activities. They either paid for satellite Internet subscriptions themselves or relied on contributions from friends and supporters abroad to cover these costs.

Samer, involved in developing live video streaming solutions and alternative Internet access devices, emphasized the lack of external support for their initiatives. He stated that his team did not receive any training or assistance. In contrast, he mentioned that some media teams did undergo training in Turkey, which was funded by American and European sources, but this was limited to individuals outside Syrian territories.

4.6. The Transformation and Decline of Cyber-Activism in Syria

In the early stages of the Syrian revolution, social media platforms were instrumental in mobilizing people, sharing ideas, and promoting the cause. However, as the conflict escalated, the dynamics shifted. The increasing arrests, deaths, displacements, and a lack of international response led to a decline in the influence of cyber-activism.

Ahmad reflected on this shift, stating, "After the first year, real-world presence became paramount, overshadowing cyber presence and activities. The impact of rallying on social media decreased while witnessing daily killings, destruction, displacement, and global silence further diminished its influence".

The period post-2012 saw a gradual shift from civil activism to militarization. Many cyber-activists transitioned to humanitarian work, assisting the growing number of displaced

70 Michelle Barrow, "Challenging Information Control with Communication Technologies in Syria", E-International Relations, 26 April 2022, https://www.e-ir.info/pdf/97189, accessed 11.08.2023.

individuals. Political rivalries, partisanship, and external interference also diverted attention from cyber-activism.

Financial constraints were another significant hurdle. Samer detailed the high costs associated with initiatives like live broadcasting, revealing that their group's efforts cost them over $200,000. Despite attempts to secure financial support, major channels like Al Jazeera declined to assist and even recruited some of their team members, weakening the group further.

Security concerns also plagued cyber-activism. The infiltration of coordination groups and leaks of protest locations to the regime resulted in arrests and detentions. This led to a loss of trust within the activist community and a shift from coordination to news dissemination and event documentation.

Despite these challenges, cyber-activism facilitated the formation of networks and personal relationships among activists. Virtual groups transformed into forums for exchanging ideas, building trust, and fostering connections. Samer and Ahmad both emphasized the transition of their virtual networks into lasting friendships and professional relationships.

In conclusion, cyber-activists in Syria demonstrated remarkable resilience and innovation in using technology to disseminate information, counter-propaganda, and maintain communication during the initial stages of the revolution. However, as the conflict intensified and challenges mounted, cyber-activism began to decline. Factors contributing to this decline included the lack of institutional support, high operational costs, state-backed cyber infiltration, and the increasing focus on real-world activism and humanitarian efforts. Despite the decline, the role of cyber-activism in shaping the narrative of the Syrian revolution and highlighting the power of digital activism in modern conflicts remains significant.

5. Cybernetic Groups: Manoeuvring Operations in Syrian Cyberspace

Amidst challenges to its authority in various regions, the Syrian regime adapted its tactics by deploying trained allies proficient in hacking and cyber-attacks to target activists. This shift transformed the cyber domain into an intense battleground, resulting in the hacking and closure of numerous social media pages and websites supporting activist causes.

According to Wilhelmsen (2014), non-state cyber-actors in Syria, both pro- and anti-government, primarily sought subversion through hacking activities. Their strategies encompassed guerrilla tactics in cyberspace, with operations classified into three categories: individual or small-group attacks, limited attacks by small groups, and coordinated attacks involving international actors. The efficacy of these cyber-actors was contingent upon organized collective actions and access to requisite resources. This evolution in cyber warfare has added layers of complexity and risk to the digital activism landscape in Syria.[71]

5.1. Anti-regime Cyber Groups

These cyber activist groups often succeeded in dominating social media narratives, even though their operations were primarily limited to defacements, DDoS attacks, and hijacking social media accounts. The major known groups are:

- **Telecommix**: As a decentralized global group of cyber-activists, it played a crucial role in assisting Syrian activists. Their technical prowess aided in bypassing government censorship, ensuring secure communication, and safeguarding the

71 Vivi Cathrine Ringnes Wilhelmsen, Soft War in Cyberspace: How Syrian Non-State Actors Use Hacking to Influence The Conflict Battle Of Narratives, Master's Thesis, University Of Oslo, Oslo, Norway, 2014,

anonymity of activists. Their interventions included the promotion of safe Internet practices, like using the Tor browser and HTTPS protocols, and the assistance in the anonymous transmission of sensitive data, such as event recordings and personal testimonies.[72] Telecommix also exposed vulnerabilities in the Syrian governmental network, identifying numerous unsecured home routers and revealing the surveillance capabilities of the regime, which had been facilitated by technology sourced from American company Blue Coat Systems.

- **Anonymous**: The decentralized and fluid nature of Anonymous enabled it to be a potent force against censorship and governmental control. This global collective has become a symbol of how 21st-century cyber-activism can challenge traditional power structures.[73] Anonymous launched cyber-attacks against Syrian government websites, exploiting their weak security measures to disseminate narratives contradicting the regime's propaganda. Notably, the "Syrian Files" operation by Anonymous, in collaboration with Wikileaks, exposed extensive communications between Syrian political figures and international institutions, revealing the complexities of global politics and the Western stance on Syria.[74]
- **Other Cyber-Activist Initiatives:** Numerous smaller and unnamed groups in the cyber domain also played pivotal roles in supporting activists. Their unorganized nature was intentional, aimed at evading regime detection and attacks. These groups managed to compromise significant websites, including the Syrian parliament's website and the pro-regime TV station "Al Donya", using DDoS attacks. A particularly significant breach was the hacking of Syrian President Bashar Al-Assad's inbox, which revealed over three thousand emails, raising serious security concerns and sparking a major scandal.[75]

5.2. State-backed Cyber Groups:

Despite stringent control measures by the Syrian regime over the cybersphere, the rise of cyber-attacks by activists prompted the regime to collaborate with third-party groups. Although these groups claimed independence, they had close ties with state agencies, especially intelligence services.

- **Syrian Electronic Army (SEA):** SEA, described as the state's digital military service, emerged as a response to counter opposition dominance online. Initially, SEA's tactics were unsophisticated, targeting social media platforms like Facebook with pro-regime content. Their attempts were largely thwarted by opposition hacktivist groups by mid-2012. However, by late 2012, SEA's capabilities improved, with members allegedly trained in Dubai and supported by Russia. They transitioned to using more advanced malware techniques, including phishing and spear-phishing, to target opposition groups and international entities. SEA's attacks resulted in significant financial losses and the acquisition of sensitive data.

72 Sahar Khamis, Paul Gold, and Katherine Vaughn, "Beyond Egypt's 'Facebook Revolution' and Syria's 'Youtube Uprising:' Comparing Political Contexts, Actors and Communication Strategies.", *Arab Media & Society*, 15:1, 2012, pp. 1-30.

73 Taylor Owen, *Disruptive Power: The Crisis of the State in the Digital Age*, Oxford Studies in Digital Politics, Oxford University Press, Oxford, 2015.

74 Julie Racicot, The Syrian Civil Conflict in the Cyber Environment, Master's thesis, Royal Military College of Canada, Kingston, Canada, 2015.

75 Diego Regalado, Nart Villeneuve, and John Scott Railton, *Behind the Syrian Conflict's Digital Front Lines*, FireEye, California, 2015.

- **Group 5:** Citizen Lab identified a cyber group, named "Group 5", operating against the opposition. The group disseminated anti-regime content through malicious emails and websites. While the group's direct ties to the Iranian government are unconfirmed, its activities suggest possible Iranian backing.[76]
- **Cyber Lebanese Group:** FireEye reported a Lebanese group conducting spear-phishing attacks against Syrian opposition accounts. This group was linked to Hezbollah's Islamic Resistance. The investigation revealed a leaked Syrian intelligence memo detailing a training program for social media activists, reinforcing the connection between SEA and the Syrian regime.[77]

State-affiliated cyber operations can be categorized into three phases:

- **Phase One (Mid-2011 to Mid-2012)**: Initial attempts focused on countering anti-regime narratives on social media and international news websites. These early efforts were largely ineffective due to the opposition's successful countermeasures.
- **Phase Two (Late 2012 to Early 2014):** More sophisticated attacks were launched, employing advanced malware and professional hacking strategies. Techniques like phishing and spear-phishing were used to penetrate opposition networks, steal sensitive data, and disrupt their activities. Attacks during this phase yielded substantial amounts of classified and sensitive information.
- **Phase Three (Late 2013 onwards):** The cyber groups transitioned into cybercriminal activities, targeting private businesses for financial gain. These attacks involved data theft, system paralysis, and ransom demands.

Overall, state-backed cyber groups have evolved over time, adapting their tactics and techniques to counter opposition narratives, acquire sensitive information, and achieve personal financial gains.

5.3. International Response to State-backed Cyber Operations

Since 2011, the U.S. and EU have imposed sanctions on individuals and entities associated with human rights violations and support for the Syrian regime. In 2012, the EU sanctioned the Syrian Minister of Telecommunication for web content control and surveillance system implementations. In 2015, the FBI listed three members of the Syrian Electronic Army (SEA) for cyber-attacks against U.S. targets. While one member, Peter Romar, was arrested in Germany, the others remain at large.

6. 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

76 Morgan Marquis-Boire, Jakub Dalek et al., "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools", Citizen Lab, 15 January 2013, https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/, accessed 12.02.2024.

77 Diego Regalado, Nart Villeneuve, and John Scott Railton, *Behind the Syrian Conflict's Digital Front Lines*, FireEye, California, 2015.

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 study 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 catalogued 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:

- **Governance Layer:** The Syrian Telecommunications Company monopolized access to the global network, regulating service providers and making technological decisions through its affiliated directorates.
- **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.
- **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.
- **Intelligence Apparatus Layer:** Security branches used the Syrian Telecommunications Company to access data, representing the regime's operational arm in the cyber sphere.
- **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. However, 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. 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.

> *"Without cyberspace, the revolution would have struggled—live streamingaided 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.*

Conflict of Interest Statement:

The author declares that there is no conflict of interest.

REFERENCES

Published Works

AL-SAQAF Walid (2016). "Internet Censorship Circumvention Tools: Escaping the Control of the Syrian Regime", *Media and Communication,* 4:1, 39-50.

APPLEGATE Scott (2011). "Cyber-militias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security & Privacy*, 9:5, 16-22.

BISWAS Masudul and SIPES Carrie (2014). "Social Media in Syria's Uprising and Post-Revolution Libya: An Analysis of Activists' and Bloggers' Online Engagement", *Arab Media & Society*, Fall 2014 (19):1, 1-21.

DE ANGELIS Enrico and BADRAN Yazan (2016). "Interacting in a Context of War: Communication Spaces in Idlib", *Confluences Méditerranée*, 99:4, 149-160.

GÖKSUN Yenal (2015). "Cyberactivism in Syria's War: How Syrian Bloggers Use Internet for Political Activism", BAYBARS-HAWKS Banu (eds), *New Media Politics: Rethinking Activism and National Security in Cyberspace*, Cambridge Scholars Publishing, 2015, 49-62.

GOSWAMI Manash (2018). "Social Media and Hashtag Activism", *Liberty Dignity and Change in Journalism*. Kanishka Publisher, New Delhi, 2018, 252-262.

HENNEFER Ashley N. (2013). Cyberactivism: A Generational Comparison of Digital Activism, Master's thesis, University of Nevada, Reno.

İLİ Burak (2023). "Bibliometric Analysis of Hashtag Activism Researches", *Turkish Online Journal of Design, Art and Communication*, 13:4, 900-915.

KHAMIS Sahar (2017). "Revisiting Cyberactivism Six Years After the Arab Spring: Potentials, Limitations and Future Prospects", Nele Lenze, Charlotte Schriwer & Zubaidah Abdul Jalil (eds), *Media in the Middle East*, 2017, Palgrave Macmillan Cham, 3-19.

KHAMIS Sahar and VAUGHN Katherine (2011). "Cyberactivism in the Egyptian Revolution: How Civic Engagement and Citizen Journalism Tilted the Balance.", *Arab Media & Society*, 14:3, 37-74.

KHAMIS Sahar and VAUGHN Katherine (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,* 4:2-3, 145-163.

KHAMIS Sahar, GOLD Paul B. and VAUGHN Katherine (2012). "Beyond Egypt's 'Facebook Revolution' and Syria's 'Youtube Uprising:' Comparing Political Contexts, Actors and Communication Strategies.", *Arab Media & Society*, 15:1, 1-30.

MANSOUR Faten A. (2015). Cyber-Activism: Engendering Political Subjects Within New Logics of Resistance in Contemporary Egypt and Yemen, Master's thesis, American University in Cairo, Cairo, Egypt.

MATTHIEU Rey (2017). "Preventing a Mobilization from Spreading: Assad and the Electronic War", Nele Lenze, Charlotte Schriwer & Zubaidah Abdul Jalil (eds), *Media in the Middle East*, 2017, Palgrave Macmillan Cham, 89-106.

McCAUGHEY Martha and AYERS Michael D. (2003). *Cyberactivism: Online Activism in Theory and Practice*, Routledge, New York.

MEHAN Julie E. (2008). *Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger*, IT Governance Publishing, United Kingdom.

OWEN Taylor (2015). *Disruptive Power: The Crisis of the State in the Digital Age*, Oxford Studies in Digital Politics, Oxford University Press, Oxford.

POWERS Shawn and O'LOUGHLIN Ben (2015). "The Syrian Data Glut: Rethinking the Role of Information in Conflict", *Media, War & Conflict,* 8:2, 172-180.

RACICOT Julie (2015). The Syrian Civil Conflict in the Cyber Environment, Master's thesis, Royal Military College of Canada, Kingston, Canada.

RADSCH Courtney (2016). *Cyberactivism and Citizen Journalism in Egypt: Digital Dissidence and Political Change*, Palgrave Macmillan, New York.

REGALADO Daniel, VILLENEUVE Nart and RAILTON John Scott (2015). *Behind the Syrian Conflict's Digital Front Lines*, FireEye, California.

SIGHOLM Johan (2013). "Non-State Actors in Cyberspace Operations", *Journal of Military Studies,* 4:1, 1-37.

WILHELMSEN Vivi Cathrine Ringnes (2014). SOFT WAR IN CYBERSPACE How Syrian non-state actors use hacking to influence the conflict battle of narratives, Master's thesis, University of Oslo, Oslo, Norway.

WOO-YOUNG Chang and WON-TAEK Lee (2006). "Cyberactivism and Political Empowerment in Civil Society: A Comparative Analysis of Korean Cases", *Korea Journal*, 46:4, 136-167.

Internet Sources

"Branch 215, Raid Brigade Military Intelligence Division", Violations Documentation Center, 2013, http://t.co/t53aZ4XbJb, accessed 3.10.2023.

"Ministry of Communication and Technology". https://shorturl.at/5yRih, accessed 14.3.2024.

"MTN Syria", https://en.wikipedia.org/wiki/MTN_Syria, accessed 12.3.2024.

"National Agency for Network Services". Establishment of the national network, https://nans.gov.sy/ar/page/establishment_of_the_national_network_se, accessed 22.03.2024.

"New Cisco Annual Internet Report Forecasts 5G to Support More Than 10% of Global Mobile Connections by 2023", *Cisco Newsroom*, 18 February 2020, 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, accessed 14.1.2024.

"Open Season: Building Syria's Surveillance State", Privacy International, December 2016, http://privacyinternational.org/report/1016/open-season-building-syrias-surveillance-state, accessed 20.11.2023.

"Russia Restructures Military Intelligence Network to Disrupt Support for Ukraine", Asharq Al-Awsat, 2024, https://shorturl.at/CglBH, accessed 24.2.2024.

"Syria: Tal al-Mallohi sentenced after flawed trial", Amnesty International, 18 February 2011. https://www.amnesty.org/fr/wp-content/uploads/2021/07/mde240062011en.pdf, accessed 24.1.2024.

"Syrian Center for Media and Freedom of Expression". Internet Media, https://scm.bz/en, accessed 5.3.2024.

"Syrian Government Orders Seizure of Assets of Rami Makhlouf", *Al-Jazeera*, 19 May 2020. https://www.aljazeera.com/economy/2020/5/19/syrian-government-orders-seizure-of-assets-of-rami-makhlouf, accessed 12.03.2024.

"Syrian Security Branches and Persons in Charge ". Syrian Network for Human Rights, https://snhr.org/public_html/wp-content/pdf/english/Syrian_security_branches_and_Persons_in_charge_en.pdf, accessed 05.01.2024.

"Syrian Telecommunication Regulatory Authority", https://www.sytra.gov.sy/index.php/en/about-us, accessed 05.02.2024.

BAIAZY Amjad. "*Syria's Cyber War"*, https://www.academia.edu/3555530/Syria_Cyber_Wars, accessed 03.02.2024.

BARROW Michelle. "Challenging Information Control with Communication Technologies in Syria", *E-International Relations*, 26 April 2022, https://www.e-ir.info/pdf/97189, accessed 11.08.2023.

CHAMPAGNE - KITETOA Antoine. "Network Surveillance: Qosmos, a Tool Provider for Syria's Leader Al-Assad", *Reflets*, 09 May 2014, https://reflets.info/articles/network-surveillance-qosmos-a-tool-provider-for-syria-s-leader-al-assad, accessed 13.01.2024.

GURULI Nino and DÁVILA-RUHAAK Sarah. "*Digital Dominion: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights*", Access Now Publisher, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Digital-dominion-Syria-report.pdf, accessed 25.10.2023

KHARROUB Tamara. "Cyberactivism in the Middle East: Six Potentials and Six Limitations of New Media Technologies in Democratization" *Arab Center Washington DC*, September 2015, https://arabcenterdc.org/resource/cyberactivism-in-the-middle-east-six-potentials-and-six-limitations-of-new-media-technologies-in-democratization, accessed 21.02.2024.

KHEOPS. "#OpSyria: When the Internet Does Not Let Citizens Down", *Reflets*, 11 September 2011, https://reflets.info/articles/opsyria-when-the-internet-does-not-let-citizens-down, accessed 13.02.2024.

LEE Bryan. “The Impact of Cyber Capabilities in the Syrian Civil War”, *Small Wars Journal*, 26 April 2016, https://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war, accessed 24.01.2024.

LEYDEN, John. “UK Firm Denies Supplying Spyware to Mubarak’s Secret Police”, *The Register*, 21 September,2011, https://www.theregister.com/2011/09/21/gamma_international_denies_egyptian_links, accessed 20.02.2024.

MARQUIS-BOIRE, Morgan, DALEK Jakub et al. “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools”, Citizen Lab, 15 January 2013 ,https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/, accessed 12.02.2024.

NEUMAYER Christina and RAFFL Celina. “Facebook for Global Protest: The Potential and Limits of Social Software for Grassroots Activism”, Paper presented at 5th Prato Community Informatics & Development Informatics Conference, Prato, Italy, October 2008, http://ccnr.infotech.monash.edu/conferences-workshops/prato2008.html, accessed 05.03.2023

TALLAA Maen. “The Syrian Security Services and the Need for Structural and Functional Change”, Omran for Strategic Studies, 18 November 2016, https://omranstudies.org/index.php/publications/papers/the-syrian-security-services-and-the-need-for-structural-and-functional-change.html, accessed 21.10.2023.