IdPS Interdisciplinary Political Studies
Number 11 Issue 2/ December 2025
ISSN 2039-8573 online
DOI: 10.1285/i20398573v11n2p471
Published by
University of Salento
Department of Human and Social Sciences

RESEARCH ARTICLE

The Evolution of Cyberauthoritarianism in Lebanon

The Case of the Lebanese National Cyber Security Strategy

Alessia TORTOLINI

University of Bologna

Abstract

This paper examines how the evolution of surveillance in Lebanon contributed to the formulation of the Lebanese National Cyber Security Strategy (LNCSS), legitimising cyberauthoritarianism. Even though the LNCSS was presented as a tool for technological advancement, it resulted in the use of cybersecurity and intelligence to repress dissent and target activism. By employing the law in context approach, this study traces the evolution of the power relations between the political élites and the oppositions in the online space and their repercussions on the physical one, focusing on how the persecution of activism and anti-governmental online content led to a redefinition of the boundaries of state's authority, both online and offline. Being activism and dissent perceived by the élites as threats to their primacy position in Lebanese politics and society and considering consociationalism as a crucial tool for the preservation of disparities among the population, the Lebanese government progressively legitimated the cyberauthoritarian discourse through *ad hoc* strategies, which eventually resulted in the LNCSS.

Keywords: Authoritarianism, Lebanon, Cybersecurity, Public policy, Cyberauthoritarianism

Introduction

In 2019 Lebanon experienced the most severe economic crisis in the history of the country. Even though the finances of the country had already been afflicted by the Syrian war, the decrease of remittances, and the arrival of Syrian refugees, since 2018 the situation was catastrophic. Furthermore, the mismanagement of the European Commission's loan exacerbated the crisis, leading to unprecedent levels of debt and currency devaluation, making it impossible for the Central Bank of Lebanon to access further loans in US dollars. Eventually, this determined a snowball effect on import and trades, as well as the Central Bank freezing citizens' accounts and pushing the country to a deliberate crisis (World Bank, 2023).

Since October 2019 rumours about the government imposing a tax on Voice Over Internet Protocol calls spread, fostering the response of the population. The long-time discontent with the clientelist politics of Lebanon, in fact, erupted in the streets, with citizens showing their mistrust towards the country's institutions and politicians (Yee & Saad, 2019). The 2019 WhatsApp protests, as they were then labelled, were unprecedented in Lebanese history, successfully paralysing the country and attracting worldwide attention on the situation. The government's violent repression of protests was condemned by international human rights associations, who denounced arbitrary arrests and the massive use of tear gas and shootings (Daher, 2021). Meanwhile, the Internet became another space

CONTACT Alessia Tortolini, Alessia.tortolini@unibo.it, Department of Political and Social Sciences, University of Bologna, Italy

of protest, with sectarian powers intervening to limit freedom of speech and targeting all those people who were identified as potential threats to the security of the state.

The definition of Lebanon as a consociational democracy helps understanding the role played by sectarianism within the Lebanese Republic, and how the intercurrent dynamics between sectarian élites shaped the institutional management of security (Dixon, 2020; Lijphart, 1969). The power struggles among the Maronites, Sunni and Shiite élites influenced the socio-political dynamics of the country and found expression in the formation of frail governments based upon alliances which have changed during the decades. By enhancing institutional and sectarian practices, each political faction sought to exploit the legal framework to protect their interests, inevitably weakening citizens' trust in the Lebanese institutions. The existence of clientelist networks within social groups is indeed pivotal for the maintenance of power by political elites (El-Masri, 2023). Clientelism has been institutionalised into both the political and economic framework and its elimination would compromise the survival of the Lebanese Republic as a whole (Hamzeh, 2001). Therefore, any form of dissent towards the preservation of the established system has traditionally been repressed by the Government.

Authoritarianism, as a means for the safeguard of the consociational order, has historically characterised Lebanese sectarian élites, allowing them to protect and progressively institutionalise their political privileges at the expenses of the population. The sectarian concentration of power, strengthened through favouritism in appointing military and governmental roles, created an *ad hoc* institutional framework to suppress dissent against consociationalism and justify repressive measures in defence of sectarian interests. Furthermore, technological advancement has paved the way for the emergence of a new confrontational arena, i.e. the cyber space, where sectarian élites have progressively extended their authoritarian rule through the development of specific surveillance strategies. Cyberauthoritarianism is in fact today one of the most efficient strategies used by Lebanese authorities to preserve the established order. Cyberauthoritarianism, grounded in the legal cybergovernance strategies used to curb online oppositions, broadens sectarian authoritarianism by leveraging digital technologies to both reinforce control mechanisms and accelerate the suppression of dissent. Put differently, authoritarianism in the cyber space intensifies sectarian practices and further institutionalise them across social, economic, and political structures.

Drawing on the legal texts concerning digital surveillance and grey literature addressing government-enabled measures of repression, this research seeks to answer the following research question: how has cyberauthoritarianism evolved in Lebanon and in what ways has online dissent been progressively incorporated into the country's cybersecurity legislation? Through the use of the law in context approach, this study examines the Lebanese legislative production on digital surveillance in relation to the evolving dynamics of dissent between opposition groups and political élites. This research assumes that ruling actors have employed legal frameworks to safeguard their privileges and suppress online dissent by reframing it as a cybersecurity threat, a tendency likely reflected in the Lebanese National Cyber Security Strategy (LNCSS). After presenting the theoretical framework, which provides a definition of cyberauthoritarianism, and outlining the methodological approach, the article will focus on analysing the development of dissent framed as a cybersecurity threat, culminating in the examination of the LNCSS.

Gewaltmonopol and its evolution in the cyber space

When discussing authoritarianism, Hannah Arendt identified specific features, such as limited political freedoms and a strong central power that operates without constitutional accountability (Arendt, 2017). Put differently, symptoms of authoritarianism can be observed whenever political systems exhibit limited pluralism due to a leader or a ruling elite exercising power without effective legal constraints, even when such limits are formally prescribed (Linz, 2000). Coercive measures are commonly employed in authoritarian political systems, especially to suppress oppositions and restrict political competition (Levitsky & Way, 2010). Therefore, the distinction between the legitimate and illegitimate use of force by the state becomes blurred, especially when those in power seek to secure their position.

The use and the misuse of *Gewaltmonopol*, the State's monopoly of the use of force, invite reflection on the spaces where the state exercises its power, and the boundaries within which that authority extends (Benjamin, 2014; Weber, 2004). Authoritarian regimes often extend their control over populations well beyond the physical boundaries of the state. A notable example involves exiles and dissidents who, despite living outside their countries' boundaries, remain subject to control by the authorities of their state of origin. This practice, common since the Cold War, has become a distinctive feature of several Middle Eastern regimes, such as those of Syria, Iran or Iraq, prompting international observers to question the dynamics of contention beyond national territory (Conduit, 2020).

Since the 2000s, States have extended their authority into a non-physical space: the Internet. The cyber space represents the latest evolution in the relationship between power and territoriality, where boundaries are drawn not to limit the State authority but to control citizens' activities. The Internet played a pivotal role during the Arab Revolutions of 2011, with social media rapidly becoming a tool employed by both authoritarian regimes and their opponents (Aouragh & Alexander, 2011). The use of Information and Communication Technologies (ICT) during the Arab Revolutions, in fact, marked a crucial turning point, not only in the development of online activism that challenged censorship and restrictions on freedom of speech, but also in providing authoritarian regimes with new instruments to consolidate their power (Al-Rawi, 2014; Allagui & Kuebler, 2011; Esfandiari, 2010).

The adaptability of authoritarian regimes to ICTs has enabled them to develop specific strategies to extend their *Gewaltmonopol* in the cyber space through legal and technological information control and by challenging opponents' narratives (Abrahams & Leber, 2021; Deibert, 2015). Put differently, the expansion of digital technologies has allowed authoritarian regimes to further consolidate their power by exerting control and repression in the online space. This phenomenon, known as digital authoritarianism, is pivotal for understanding how the relationship among the State and society has evolved, as ICTs are used both to enhance repressive strategies and to spread dissent against authoritarian practices (Pearson, 2024; Dragu & Lupu, 2021). One of the main pillars of digital authoritarianism is the encouragement of self-censorship among the population, used as a tool for facilitating large-scale suppression of online dissent. This system can either collapse or intensify depending on the clarity of the boundaries that define acceptable speech: when such boundaries are absent or too weak, it can trigger the so-called cyber-speech cascade (Druzin & Gordon, 2018). The expansion of authoritarian regimes' *Gewaltmonopol* into the cyber space, then, is closely dependent on the existence of boundaries, which are established through specific legislation. However, such laws are often intentionally vague and verbose, designed to instil a climate of intimidation and fear (Druzin & Gordon, 2018; Deibert, 2010).

Furthermore, dissent and opposition movements are increasingly framed by authoritarian regimes as potential threats to their survival, making the implications of digital authoritarianism particularly evident in matters of national security. By shaping the concept of national security according to their interests and goals, authoritarian regimes have developed *ad hoc* cyber security strategies that contribute to model the on-line space after the physical one, thereby enforcing regulations and policies to control the 'cyber borders' (Deibert, 2015). Building on the concept of digital authoritarianism, this paper considers cyberauthoritarianism as the expansion of legal boundaries in the online space under the pretext of safeguarding national security. By considering digital authoritarianism as a sociopolitical model consisting of three components, i.e. the use of digital technologies to surveil and repress; the deployment of authoritarian practices in the cyber space to influence and control narratives; and the regulation concerning digital systems (Jarrett et al., 2025), this paper puts forward the definition of cyberauthoritarianism as a strategy of cybergovernance through which governments protect their hold on power by enacting legal frameworks that target online opposition and facilitate the legal repression of dissent in both digital and physical spaces. This framework focuses on how authoritarian regimes construct legal justifications to physically target opposition and dissent originating in the cyberspace by framing them as threats to national security, thus modelling cybersecurity to pursue subjective goals. They do so by developing specific laws and regulations that enable ruling élites to physically persecute and repress activists and dissidents through the expansion of their *Gewaltmonopol* in the online space, all without accountability.

Even countries that are democracies *de jure* can present authoritarian traits that further developed in the cyber space. The case of Lebanon is, in that sense, particularly emblematic of this tendence. Since its independence, Lebanon saw the emergence of élites who strengthen their position through clientelism. Notwithstanding the alternation of Sunnis, Maronites and Shi'ites at the top levels of the State, any faction relied heavily on the presence of networks of loyalists to exercise their authority (Arnous, 2018). Furthermore, given the influence of sectarianism in the institutional development of the country, the institutional framework foresaw the implementation of a quota system with the presence of coalition governments (Salamey, 2021; Di Peri, 2009; Lijphart, 2002). The survival of governments therefore remains firmly anchored to the presence of clientelist networks embedded within the State apparatus, particularly given the quota system's reliance on the functioning of clientelism. In this context, Lebanese political élites actively sustain sectarianism, which is deeply intertwined with clientelist practices, despite publicly denouncing it as a root cause of the instability of the country. This critique, however, mirrors the discourse advanced by opposition groups and civil society actors, which the political élites seek to appropriate in an effort to maintain legitimacy and control over the narrative (Abi Yaghi & Yammine, 2020; Nagle, 2018).

Similarly to what happened during the Arab Revolutions, the use of artificial intelligence tools, on-line surveillance, and manipulation of information on social media had a direct effect on exploiting national security as a justification for the survival of authoritarian regimes (Conduit, 2024). In the Lebanese context, political élites have sought to safeguard their power position and their economic privileges by redefining the legal boundaries to their *Gewaltmonopol* in the cyber space. This has involved the introduction of a targeted legislation aimed at reframing cybersecurity, where online dissent is portrayed as a threat to national security, namely the Lebanese National Cyber Security Strategy (LNCSS). The latter builds upon prior legislation concerning the regulation of communications and digital privacy, particularly regarding economic matters. The economic sector, heavily controlled by sectarian groups, has become the primary target of oppositions forces, as it is widely perceived as the expression of the systemic corruption in the country (Deets & Abou Harb, 2024; Majed & Salman, 2019). The wave of criticism erupted in 2015 was met with massive repression by the government, while the economic crisis of 2019 further intensified the use of ICTs and social media by both protesters and political élites (Abi

Yaghi & Yammine, 2020). However, while protesters employed these tools to mobilise and disseminate their demands, political élites exploited them to monitor and suppress dissent through targeted surveillance and physical repression.

Methodology

In order to retrace the development of cyberauthoritarianism in Lebanon and its effects in society, this study employed law in context to identify the relation between power relations and cybersecurity tools in regard to their effects on civil society, activists and minorities. Law in context, in fact, revealed to be particularly efficient in analysing the social dimension of the law and its effects, also paying attention to the relationship between informal rules and norms existing within a community (Hart, 1961; Twining, 1997). Arising from the field of socio-legal studies, law in context allows for the understanding of the origin and the evolution of laws and legal frameworks, taking into account how historically institutions and political discourses are intertwined, providing fertile ground for the exercise of power by the ruling élites (Twining, 2000, 2007, 2009).

Specifically, law in context facilitates the analysis of primary sources, namely legal texts, in relation to secondary sources, hence fostering an interdisciplinary approach to the study of legislative development. The case study of Lebanon was therefore constructed as it follows. As primary sources, two laws were considered, i.e. Law no. 140/1999 and Law no. 81/2018, as well as the LNCSS, a strategy, and thus an infra-legal instrument developed by the Government, which is here treated as a norm since it legitimised provisions that had been applied even prior to its formal enactment to serve the shared interests of sectarian leaders (Lascoumes & Le Gales, 2007). In legal terms, a strategy can be considered as a norm when it influences decision-making without parliamentary discussion, formalising practices that were already occurring and granting them institutional legitimacy. Primary sources were interpreted in light of both historical events and secondary sources, which in this case study are represented by reports, indicators, and information concerning the respect of human and digital rights in Lebanon, with a specific focus on repression mechanisms employed by the government. In particular, secondary sources included grey literature produced by international organisations advocating for human and digital rights (including Muhal - Observatory for Freedom of Expression, Electronic Frontier Foundation - EFF, Global Voices Advocacy - AdVox), independent media platforms such as Open Democracy, and international and Lebanese NGOs (Amnesty International, Human Rights Watch, Freedom House, Social Media Exchange - SMEX). In this regard, the law in context approach helps shed light on how historical events and political decisions influence legislative development, eventually focusing on the LNCSS as both the outcome of the legislative evolution in the field of cybersecurity and the tool for the exercise of cyberauthoritarianism. More specifically, the analysis has been divided into the following sections: the historical examination of Lebanese power relations, with a focus on the relationship between consociationalism and authoritarianism; the analysis of the evolution of the legal framework on cyber security; the examination of the use of cyber surveillance up to 2019; and the in-depth analysis of the LNCSS.

Authoritarianism and consociationalism

Consociationalism has traditionally been employed to classify all those countries characterised by divided societies, where the institutional framework and the political composition of the state are designed to promote peace amid ongoing conflict among different social groups (Lijphart, 1977). This classification highlights the existence of social divisions among society, which must be maintained in order to ensure the establishment of a form of political segregation aimed at preventing conflict through the rule of an élite

(Dixon, 2020). According to this perspective, a power-sharing system based on proportional representation is regarded as the essence of consociationalism as the only viable means of ensuring democracy in divided societies. Therefore, the need to prevent or resolve conflicts is used to justify the establishment of an institutional framework that, in the case of Lebanon, guarantees the reproduction of sectarian dynamics in accordance with the law enforced by sectarian authoritarian élites (Dixon, 2020). In this sense, authoritarianism and consociationalism are two sides of the same coin, as the former is the conflict management tool of the latter.

The Lebanese constitution's *de facto* protection of sectarianism allowed sectarian élites to repress dissent through authoritarian means while escaping accountability, thereby reshaping consociational discourse in ways that served their needs. Proportional representation is fundamental in enabling sectarian élites to sustain their clientelist network and to safeguard their control over the economy of the country through a "sectarian authoritarian form of power-sharing" (Dixon, 2020, p. 124). Furthermore, the Constitution defines Lebanon as an Arab country, thereby aiming at establishing a common identity in the declared intent to overcome sectarianism in the aftermath of the civil war (1975–1990) (Salamey, 2021). However, the constitutional revision that followed the Ta'if Agreement was no other than a cosmetic operation, since political parties continued to forge alliances based on confessional affiliations, keeping sectarianism alive to fulfil their political goals (Mazzola, 2023; Halawi, 2020). Inevitably, alliances impacted on the appointment of ministries and, consequently, on the so-called service ministries, namely the most funded ones, which inevitably underwent the influence of sectarian and clientelist dynamics (Mahmalat & Zoughaib, 2022; Toubia et al., 2019). Although this aspect may seem marginal, it proves to be crucial when the government allocates funds, choosing to invest in certain activities over others. This mechanism inevitably ensures that, through consociationalism, resources remain in the hands of sectarian élites, securing not only wealth but also significant political influence.

The growing social and political instability that had gripped the country since the Cedar Revolution worsened in the aftermath of Arab Revolutions and the Syrian war. Maintaining sectarianism alive was pivotal for the survival of the consociational system, with the ruling political parties exploiting the institutional framework of the country to secure and reinforce their position of power (El-Masri, 2023; Di Peri, 2014). The issue at stake, then, implied the necessity of safeguarding economy by keeping it firmly in the hands of élites. Indeed, this phenomenon was closely connected to the intensification of clientelist practices within the government, which contributed significantly to the mismanagement of Lebanon. Popular dissatisfaction with political corruption grew steadily, peaking with the garbage crisis of 2015, which triggered the emergence of the *You Stink!* protests and the following violent clashes in Beirut (Yee & Saad, 2019). The garbage crisis marked a point of no return in the State-society relations. Over time, the situation deteriorated further, as deepening socioeconomic disparities and fiscal deficits were exacerbated by sectarian forces manipulating economic structures through an allied entrepreneurial bourgeoisie. The collapse of the tourism sector following the onset of the Syrian civil war further compounded Lebanon's economic decline. Additionally, the governmental paralysis of 2014 revealed what Kraidy (2016, p. 21) defined as the "decapitated body politic", a condition made manifest through the State's inability to respond effectively to the garbage crisis and the popular mobilization it provoked (Harvie & Saleh, 2008; Di Peri & Costantini, 2023).

The need to preserve elitist economic privileges, as the cornerstone for the survival of the consociational order, profoundly shaped the entrenchment of sectarian authoritarianism in Lebanon. Since the independence of the country, sectarianism has been sustained by authoritarian practices that have prevented the formation of democratic institutions and effective popular participation in the management of Lebanese economic resources. In this sense, conflicts among sectarian élites functioned to counter the emergence of a cross-class revolutionary movement through structural violence and coercion (Mazzola, 2023; Halawi, 2020). Authoritarianism, legitimised by the Lebanese institutional framework set up by sectarian élites, thus became the tool for maintaining class interests and economic power (Salloukh et al., 2015). The grassroot and non-sectarian nature of the 2015 protests highlighted widespread public discontent with Lebanon's political and economic situation, while concurrently questioning the legitimacy of the government's exercise of *Gewaltmonopol*, which framed political dissent as a threat to the survival of the consociational order (Daher, 2021). The protests denounced that the very political forces dependent on sectarianism and systemic corruption for their survival might attempt to exploit the anti-establishment discourse to manipulate the outcome of administrative and political elections (Mazzucotelli, 2020). These suspicions were later substantiated with Hezbollah launching an anti-corruption campaign, whose goal was to lift the restrictions imposed by the Lebanese Central Bank on their satellite activities and affiliated networks rather than to promote a successful systemic reform (Salloukh, 2020). Since 2015, civil rights have increasingly become under threat, with activists and journalist being targeted by security forces and government supporters, and the Parliament exploiting social unrest to prolong its mandate until 2018 (Vértes et al., 2021).

Furthermore, early signs of the impending economic crisis had already emerged, with unemployment rates escalating quickly and the Central Bank imposing restrictions on access to credit for depositors. Physical and on-line spaces for dissent increasingly came under the control of the government and its supporters, marked by the intensification of repressive measures (Daher, 2021). The 2019 protests highlighted how consociationalism was *de facto* sustained by sectarian authoritarianism, as proved by the governmental attempts to reframe the discourse on sectarianism as the root cause of Lebanon's instability, while simultaneously relying heavily on repression against those who publicly denounced sectarian corruption.

The evolution of the legal framework on online security and the development of online surveillance

The Lebanese security apparatus was developed by the sectarian élites in response to the need to maintain stability in the aftermath of the civil war. Before the Ta'if agreement, there was no specific reference to security policies in the Lebanese institutional framework, with the exception of exceptional circumstances due to external threats to territorial integrity. The authority over security policy was vested in the President of the Republic, while, according to the Legislative Decree no. 102/1983, the Supreme Defence Council (SDC) was the body responsible for planning defence and security policies in cases of extraordinary circumstances or war. Legislative Decree no. 101/1984 further developed the institutional security architecture by granting the Council of Ministers the authority to supervise and implement security policies, thus making the SDC and the Government the primary source of security decision-making (Tlais, 2013).

The Ta'if agreement reorganised the security framework of the country by establishing agencies under the authority of the Ministries of Defence and Interior, whose management was distributed among sectarian leaders in order to reinforce consociationalism. By granting the Government the duty of formulating security policies, while assigning the President of the Republic with the role of Commander in Chief of the Lebanese Armed Forces (LAF), whose interventions were, however, subjected to governmental control, the Ta'if agreement effectively placed the development of a national security strategy entirely in the hands of the executive power and, *de facto*, in those of sectarian interests. The LAF, commanded by Maronites and Druze, were entrusted with the task of ensuring military surveillance which, however, was not limited to strictly military threats but also extended to domestic surveillance. All other agencies operated under the authority of the Ministry of Interior. While some of them had existed before 1991, as in the case of the General Directorate for General Security (GDGS) and the Directorate of State Security, the establishment of the Internal Security Forces (ISF) marked a significant turning point in strengthening sectarian control over the Lebanese population. This becomes particularly clear when considering that the ISF were commanded by Sunnis, the DGSG was a collective consociational leadership body which, by 1988, also included Shiites, and the Directorate of State Security was commanded by the Greek Orthodox (Tlais, 2013; Collelo, 1989).

Eventually, the LAF and the ISF became the two main pillars sustaining the security apparatus which, however, by the end of the 1990s, still lacked a proper strategy for monitoring telecommunications and cyber activities, which extended not only to politicians or community leaders, but also to common citizens. The Government's capacity of developing *ad hoc* conditions to extend its legitimate control on public affairs can in fact be traced back to the enforcement of two laws: Law no. 140/1999 and Law no. 81/2018. Given that the legal panorama of Lebanon lacked a specific regulation concerning ICTs until the enforcement of the LNCSS, these two laws provided the initial framework for the development of a national cyber security strategy that, up to that moment, was lacking.

Law no. 140/1999[1] established the right to secrecy of communications subject to exceptions in the context of explicitly issued judicial inquiries. Articles 2 and 3 delineated the limits of the judicial authorisation, restricting interception measures to cases of emergency or individuals explicitly suspected of criminal activities. The methods of interception, as well as the type of communication tools targeted, must be clearly defined, with the duration of the imposed measures not exceeding two months (L. 140/1999, Art. 2-3). However, exceptions were allowed in case the Ministries of Defence and Interior, upon receiving prior written authorisation from the Prime Minister, required an interception for very specific felonies, such as crimes against the State, terrorism, organised crime and State security. (L. 140/1999, Art. 9). Any unauthorised interception was subjected to prosecution under the penal code (L. 140/1999, Art. 17).

Moreover, Law no. 81/2018 was conceived to provide a legal framework for electronic transactions and data protection. It regulated electronic signatures, the protection of individual privacy, commercial activities, and e-commerce transactions[2]. According to the law, ICTs must not infringe upon individual freedom, especially in terms of personal identity, individual rights and privacy (L. 81/2018). While all public communications must comply with national security laws and to the Constitution, in situations involving national threats or criminal activities, the law permitted searches and seizures of personal data, financial, economic or managerial files (L. 81/2018).

The strategic importance of the ICT sector became evident with the establishment of the Lebanon Cyber Crime Bureau in 2006 by the ISF. Not formally conceived as an official branch of the Security Forces or as an agency under the authority of the Ministry of Interior, the Bureau came into force as an unofficial interrogatory body operating outside Lebanese legislative framework managed by the ISF. Its mandate and operations were not grounded into statutory law, thereby bypassing the provisions of Law no. 140/1999 and

[1] Full text of the law 140/1999: http://www.legallaw.ul.edu.lb/Law.aspx?lawId=198664, last accessed 21 July 2025.

[2] Full text of the law 81/2018: https://alp.unescwa.org/legislations/law-81-2018-electronic-transactions-and-personal-data, last accessed 21 July 2025.

exploiting the legal vacuum regarding the data protection in electronic communication (Frangieh, 2013; Abi Ghanem, 2017). The Bureau, then, functioned as a *de facto* authority with exclusive jurisdiction over social media surveillance, despite lacking formal governmental or ministerial authorisation. Consequently, its actions fell outside both institutional accountability and democratic oversight.

Furthermore, the IT industry became strongly intertwined with politics as well. The diffusion of smartphones at end of the 2000s, in fact, determined a significant increase in attention to ICTs, particularly in software development. The ICT sector grew exponentially over the last decade, with Lebanon emerging as a regional technology exporter (Ben Hassen, 2018). The establishment of the National ICT Strategy Coordination Unit in 2010, under the supervision of the office of the Prime Minister, was in fact symptomatic of the importance the government attributed to technology, even though the latter admitted to insufficiently funding academic research on the topic (Gaillard, 2010). As a result, the ICT sector developed largely through venture capital and private financial support, which in turn deepened the government's dependence on the private sector. The relationship between the public and private sectors, in fact, has long been a crucial issue for the Lebanese governments, especially since the private sector constitutes approximately 70% of the national income[3]. Put differently, when it comes to cyber security, public institutions heavily rely on the support of private entities. According to the 2017 report of the Investment Development Authority of Lebanon (IDAL), IT companies and related activities reached around 800 units (IDAL, 2017). The ICT industry appear to be particularly remunerative due to its operational model, which aligns with the traditional business model of the country based on entrepreneurial bourgeoisie composed of networks of family-run enterprises (Ahmed & Julian, 2012).

The collusion between political élites and private companies on online surveillance became particularly evident with the eruption of the Dark Caracal scandal in 2018. The Electronic Frontier Foundation (EFF), an international non-profit digital rights group, and Lookout[4], a US-based cybersecurity company, exposed one of the biggest cyber espionage campaigns in recent years, whose origin was traced back to the GDGS building in Beirut in 2012 (Lookout & EFF, 2018). Dark Caracal was a malware tool designed to access smartphones and laptops, stealing personal data from a broad range of targets, including military personnel, journalists, and civil society activists, in more than 20 countries. Despite international human rights groups and associations, such as Amnesty International, accusations of State-led cyber surveillance targeting Lebanese activists within and outside the boundaries of the country, the Lebanese government and the GDGS denied any involvement in the Dark Caracal scandal (Lookout & EFF, 2018; SMEX, 2018a, 2018b).

Cyber surveillance and physical repression up to the 2019 protests

According to human and digital rights groups like Social Media Exchange (SMEX) and Global Voices Advocacy (AdVox), the Lebanese government has repeatedly exploited online surveillance to target activists and civil rights defendants since 2015. The *You Stink!* protests marked a new era in Lebanese history due to the strength of civil society in challenging the power system dominated by sectarian élites. Unlike the past, there was widespread consensus on the identification of sectarian networks, and not political parties, as the root cause of the country's mismanagement (Assi, 2021; Daher, 2021; Abi

[3] https://www.presidency.gov.lb/English/LebaneseSystem/Pages/OverviewOfTheLebaneseSystem.aspx, last accessed 26 November 2025.
[4] https://www.eff.org/it, last accessed 26 November 2025.

Yaghi & Yammine, 2020). Furthermore, the diffusion of smartphones and portable ICT devices provided opposition groups with faster and more effective means of communication. At the same time, these technologies were exploited by the Cyber Crime Bureau to enforce surveillance over the population. This issue was closely scrutinized by SMEX and AdVox, who uncovered evidence of collusion between the ISF, the Bureau, the Lebanese Army, and the surveillance company Hacking Team in monitoring activists' communications and targeting Lebanese citizens by exploiting a bug in the Angry Birds game application (AdVox, 2015a). In other words, since 2015, opposition groups, activists, and minorities have been subjected to continuous surveillance, with the Cyber Crime Bureau conducting interrogation and making arrests without official orders by the government or the Ministry of Interior (AdVox, 2015a, 2015b). The Muhal Observatory for the Freedom of Expression reported 86 cases in 2015 alone, including interrogations, arrests, detentions, and seizures of material, with the average number of cases remaining steady through 2020 (Muhal, 2024).

The trend of the exploitation of the lack of a legislation on digital rights as the legal justification for the exercise of violence by the State intensified throughout the following years, resulting in the progressive erosion of human rights and freedom both within and outside the online space. Lebanese élites promoted counter-narratives aimed at silencing the *You Stink!* movement and delegitimising protesters' demands, as civil society organisations had been considered a threat to the stability of the sectarian power system since 2005 (Clark & Salloukh, 2013). The massive physical violence used by Security Forces to suppress the 2015 movement was followed by an increase of online surveillance measures and mobile devices remote control (Assi, 2021; Geha, 2019; Amnesty International, 2015). Social networks came under systematic control due to their pivotal role in enabling opposition movements and civil society organisations to regroup and actively participate to the 2016 municipal elections (Assi, 2021; Geha, 2019). Meanwhile, blocks of internet contents and apps paved the way for the progressive crackdown on freedom of speech, which became evident since 2017.

Under the guise of security matters, in 2017 the Minister of Telecommunications Jamal Jarrah initiated procedures for imposing biometric registration for the purchase of prepaid sim cards without proper regulations for the safeguard of personal data (SMEX, 2017a). This decision raised concerns as it followed the introduction of biometric residence permits for non-Lebanese residents in Lebanon, suggesting a clear government attempt to control both the population and the freedom of speech by restricting access to communication tools. Furthermore, attacks against activist and minorities increased, as proven by the blocking of the dating app Grindr, the cancelation of the Beirut pride, unauthorised access to WhatsApp profiles, and the arrests and interrogations conducted by the ISF (Chamas, 2023; Abdel Khalek, 2020). Amnesty International reported that the ISF forced detained activists into signing false confessions and illegal pledges to be cleared of charges, while arresting anyone who shared material online, including satirical content, criticising the ruling élite (Amnesty International, 2018a). A particularly illustrative example of this phenomenon was the arrests of Youssef Abdallah in 2018, a minor who used a meme of President Michel Aoun as his WhatsApp profile picture. He was held in detention for 38 hours without access to a lawyer, and his parents were barred from attending the interrogation (Amnesty International, 2018a; Muhal, 2018). Other notable illegal detentions included Ghassan Abdallah, general director of the Palestinian Human Rights Organisation, and Hadi Damien, spokesperson of the Beirut Pride, as well as 62 reported arrests of artists, activists and journalists in 2018 (Amnesty International, 2018b, 2018c; Human Rights Watch, 2018a, 2018b).

The protests of 2019 marked a further escalation in the State's use of violence due to a shift in the spatial dynamic of the conflict between civil society and political élites. The critique of the political-economic system, in fact, brought together several issues, such as human rights, gender inequality, unemployment and labour conditions, shedding light on the crisis of political legitimacy that sectarianism was experiencing (Sharp, 2023; Open Democracy, 2019). When the 2019 protests broke out, images of the violence perpetrated by the Lebanese Security Forces went viral, with social media serving as the primary communication channels and hashtags acting as powerful collective calls for mobilisation (Abi Yaghi & Yammine, 2020; Amnesty International, 2019a, 2019b). Online monitoring and physical violence became strongly intertwined, with the former enabling the actions of the Cyber Crime Bureau, and the latter serving both to control public spaces and facilitate on-site monitoring of mobile devices by the ISF (Daher, 2021; AdVox, 2020; Freedom House, 2020). Lebanese authorities turned to the legislation against defamation to justify the arrest of civil society members, while the Bureau continued to operate without any official mandate from the government, targeting Facebook and Twitter content related to the country's economic situation, deemed a threat to institutional security (Freedom House, 2020). The final stage of the evolving power relation between civil society and political élites was the drafting of the first national strategy for cyber security, which was supposed to fill the normative gap on the topic. Indeed, the exploitation of the concept of security by the Lebanese government led to the creation of a legal framework that both legitimised online surveillance and strengthened the capacity of law enforcement and police activities to prevent and prosecute cybercrimes.

The Lebanese National Cyber Security Strategy: Power-discourses through cyber security

The Lebanese National Cyber Security Strategy[5] (LNCSS) was developed in 2019 under the cabinet of Saad Hariri. Although the LNCSS was launched on 14 December 2022, many of the measures outlined in the strategy had already been in force long before 2019. Put differently, the LNCSS served to provide legal legitimacy for certain repressive practices already in use within the Lebanese cyberspace. The LNCSS was conceived as a policy document intended to establish a legal framework for the creation of the National Cyber Security Information System Agency (NCISA), an agency attached to the General Secretary of the Higher Council of Defence, tasked with coordinating efforts with Law Enforcement Agencies (LEA), the ISF, the Cyber Crime Bureau, and various Ministries. The strategy document consists of a Preamble written by former Prime Minister Hariri, two programmatic parts, and the Conclusions paragraph.

The first part of LNCSS is dedicated to the definition of the core pillars of the Lebanese national strategy, focusing on the country's relevant actors and the threats that would most likely affect the stability of the State. These threats are identified as "malicious cyber activities [that] are designed to compromise the confidentiality, the integrity, and the availability of Networks, IT Systems, and Information" (LNCSS, 2019, p. 13). They are classified as crimes, threats, or attacks according to the use of ICT devices, the scope of the activity, and the actors involved. Accordingly, the LNCSS categorises a range of cyber-related offenses based on their specific characteristics. Both cyber-dependent and cyber-enabled crimes, for instance, imply the use of ICT devices to perpetrate the felony, while they differ in purpose. The former typically pursue financial gain; the latter encompasses a broader range of violations, from propaganda to espionage. Indeed, terrorist threats

[5] Full text of the LNCSS: http://www.pcm.gov.lb/Library/Files/LRF/tamim/Strategie_Liban_Cyber_EN_V20_Lg.pdf, last accessed 26 November 2025.

represent the broadest category, with hacktivist threats as a subcategory. The list also includes State and State-sponsored threats as well as insider threats (LNCSS, 2019, pp. 13-14).

Furthermore, the LNCSS identifies the Government, Businesses and Organisations, and Individuals, namely citizens, consumers, and employees, as the main actors responsible for "securing the national cyber space" (LNCSS, 2019, p. 19). Notwithstanding the State retaining primary responsibility, the protection of national interests, namely the economy and cyber and non-cyber critical infrastructures, must be a multidimensional effort. This requires: the government to actively cooperate with key Ministries, LEA, and the regulatory bodies of the banking sector; organisations and businesses to safeguard the personal data they hold; and individuals to take responsibility for protecting their personal hardware (LNCSS, 2019, pp. 19-20).

The first part of the LNCSS then introduces eight strategic pillars of the national strategy for cyber security, which included: 1. Defend, deter, and reinforce against internal and external threats; 2. Develop international cooperation in the field of Cyber Security; 3. Continuously enhance State capacities to support the development of information and communication technologies; 4. Promote educational capacity on the Lebanese territory; 5. Promote industrial and technical capacity; 6. Support the export and the internationalisation of cyber security companies; 7. Strengthen collaboration between the public and the private sectors; 8. Promote the role of security and intelligence services and the strengthen of mutual cooperation and coordination with the supervision of the higher authorities (LNCSS, 2019, pp. 21-34). The first part of the LNCSS concludes by outlining the main objectives of the national strategy, among which the most important can be identified in the cooperation between the government and the private sector, the development of an *ad hoc* juridical framework to deal with the emerging cyber threats, the improvement of citizens' knowledge on cyber threats, the strengthening of LEA activities, and the development of a proper strategy to counter propaganda and destabilisation (LNCSS, 2019, pp. 35-38).

The second part of LNCSS describes the NCISA and the legal framework within which it operates. The duties of the NCISA are outlined as follows: setting policies and procedures; developing plans of action; access and counter vulnerability and threats; promote awareness; and defining critical infrastructures and operators (OVI). As the entity responsible for security in the field of information, NCISA works jointly with LEA and relevant Ministries to implement *ad hoc* national-level response teams (LNCSS, 2019, pp. 40-42). The NCISA operates at the public level, ensuring that businesses, companies, and individuals have access to defence measures. The agency also participates in academic education and research, and monitors the development of information security systems. Ultimately, the most critical activity of the NCISA is protecting against cyber threats. This requires a specific legislation, the formulation of which falls under the agency itself (LNCSS, 2019, pp. 44-45).

The examination of the LNCSS reveals two intertwined patterns that have enabled the Lebanese élites to safeguard their position of power: the role of the institutional framework in strengthening sectarianism and corruption, and a redefinition of the concept of threat. By critically engaging with these two trends in light of existing knowledge about the socio-political context, it becomes possible to shed light on how the defence of economic interests is embedded in the power discourse of Lebanese élites, as well as in their exploitation of *Gewaltmonopol* to protect those interests.

The LNCSS opens with a critique of Lebanon's sectarian conflict, presenting it as the main reason the country continues to be considered internationally a corrupt nation. Sectarianism is framed by Lebanese authorities as source of instability and a cause for social unrest, with the "multiplicity" of sectarian groups viewed as potentially exploitable for destabilising actions (LNCSS, 2019, p. 9). In contrast, corruption, as a concrete factor of public distrust towards institutions, is only briefly addressed, and primarily in opposition to digital economy and to the State-led transition to cyber progress (LNCSS, 2019, pp. 46, 9). When discussing the relationship between the institutional framework, sectarianism and corruption, the LNCSS emphasised the establishment of a cyber security sector managed jointly by the government, the private sector, and academia as pivotal for developing effective cyber security tools. To this end, the government pledges to promote public contracts with private companies and offers monetary incentives (LNCSS, 2019, par. 3.7). This explicit comment is supported by more implicit statements throughout the LNCSS, such as designating businesses and organisations as key actors for the development of a national cyber security strategy, and identifying private cyber security companies as relevant stakeholders, basically defending entrepreneurial bourgeoisie's interests (LNCSS, 2019, pp. 19, 31). It is worth noting, however, that despite the primacy given to the private sector, the State, as the overarching institutional framework, retains its role as the ultimate coordinator and overseer of the development of the LNCSS (LNCSS, 2019, p. 35).

Furthermore, the primary role of the State is emphasised not only through its coordination of cooperation among LEA, government institutions, and key ministries, but also in efforts to improve the effectiveness of LEA in prosecuting high-profile cyber-attacks (LNCSS, 2019, pp. 19, 26). Law-enforcement capabilities are presented as the institutions' primary instrument of action, especially in the implementation of technical and judicial defence mechanisms against cyber-criminal activities. This includes, among other measures, private sector-sponsored training for officials, critical stakeholders, and judges, all conducted under the supervision of State authorities (LNCSS, 2019, pp. 23, 25-26, 27-28, par. 3.8). While the independence of LEA, public officials and the banking sector is affirmed, the collaboration of "the country" with critical stakeholders is essential for the full implementation of the national strategy for cyber security (LNCSS, 2019, pp. 30-31).

The definition and acknowledgement of threats by the Lebanese institutional framework reveal varying degrees of clarity regarding what constitutes a cyber-criminal activity when perpetrated by citizens. As a matter of fact, paragraph 1.2 of the LNCSS lists propaganda as a prosecutable threat, directly associating it to cyber-enabled crimes, terrorism, and hacktivist threats, yet failing to provide any concrete examples of what such propaganda activities entail (LNCSS, 2019, pp.13-14, 37). Notwithstanding the vagueness of the concept of propaganda, the NCISA collaborates with LEA in prosecuting cyber-crimes to counter domestic activities associated with radical thinking and behaviour on the cyber space (LNCSS, 2019, p. 43). Although radical thinking is not listed in paragraph 1.2, it appears to be connected to the "hunger" of the generation raised in the 2000s, a generation that rejected the "pre-war Lebanese culture built on integrity, respect, and competence" and now seeks compensation (LNCSS, 2019, p. 9).

In the final part of the LNCSS, the presence of non-Lebanese regular and irregular migrants, workers, and job seekers in the country is framed as problematic due to their involvement with NGOs and the perceived lack of government oversight (LNCSS, 2019, p. 47). This group, in fact, is viewed as potentially vulnerable to cyber-attacks and as a "platform for potential cyber threats and other cyber criminal acts" (LNCSS, 2019, p. 47).

Ultimately, the LNCSS effectively uses propaganda as a broad category encompassing both terrorism and any discourse of dissent, thereby implicitly framing the latter as a significant threat to domestic security. As stated in the LNCSS objectives, security and defence bodies are mandated to counter propaganda and cyber incidents, including "radical thinking and behaviour related to cyber space" (LNCSS, 2022, pp. 37, 43).

Propaganda is thus associated with dissent understood as radical thinking, and legally framed as a felony. Similarly, hacktivism is criminalised, as it is defined as "the use of computer technology to promote a political agenda or a social change" (LNCSS, 2022, p. 52). These definitions are crucial because they legitimise all those violent practices of surveillance and repression enforced prior to 2019 by providing an *ad hoc* legal framework, effectively shaping domestic security policies that justify violent means of repression both online and offline.

The impact of cyberauthoritarianism from 2019 to its institutionalisation

The procedures institutionalised with the LNCSS were the result of the practices implemented since 2019, specifically targeting groups considered dangerous due to their activism or minority status. The creation of specific offences related to anti-establishment propaganda emerged in response to public criticism directed at sectarian élites, particularly from journalists, civil society organisations, and LGBTQAI+ groups. Over the years, these categories of people incurred into investigations and repression in the physical space. However, by 2019 the space for contestation and dissent had expanded into the cyber space, immediately followed by the control and repression mechanisms operated by the government.

Private telecommunication companies have become increasingly involved in controlling the access to content deemed problematic by the government (Freedom House, 2020, 2021, 2023). According to the Lebanese legislation on telecommunication, mobile companies are State-owned, despite being privately managed. This hybrid system is strategically beneficial for the State, since it allows for both consistent revenues and political oversight on telecommunications, especially considering that management contracts were often awarded on the basis of political affiliation. The cases of Alfa and Touch, the main mobile companies of the country, blocking access to Google Firebase and other Google-owned platforms since 2017 clearly illustrate this issue. The situation has worsened since 2020, with the government's complete acquisition of these companies, which are now managed by the Ministry of Telecommunications (Freedom House, 2023; SMEX, 2017b). This shift has prevented activists from putting online anti-governmental content and using the online space to raise criticism and call for rallies.

Furthermore, given the role of social networks in disseminating content about violence by Security Forces and corruption within Lebanese institutions, the Bureau intensified its monitoring of Facebook and Twitter posts. This included launching LGBTQAI+ hate campaigns online with the support of the Ministry of Telecommunications and Hezbollah supporters, as well as orchestrating online and offline harassment of minorities and activists (Freedom House, 2020, 2021). Among the most well-known examples of social media surveillance in 2020 were the cases of Saeed Abdullah and Leen Thaini, summoned by the Bureau and eventually arrested for their Facebook posts criticising President Aoun and the Ministry of Culture, respectively (Muhal, 2020a, 2020b). To this day, the Muhal Observatory for the Freedom of Expression reports dozens of ongoing cases of government critics whose opinions have been considered harmful to public morals and national security (Muhal, 2024).

After the publication of the LNCSS, groups that had already been targeted by institutions for their offline and online criticism of the corruption of the State faced further restrictions on their freedom of action and additional violations of their rights. The 2024 Israeli invasion of Lebanon further worsened the situation. Regardless of the mobile network they were using, Lebanese citizens received SMS and WhatsApp messages throughout the conflict containing threats, false information, or request for information. Inevitably, NGOs and pro-Palestine activists were specifically targeted (SMEX, 2024a). A related development involves the suspension of mobile network access for Syrian refugees, presented as a security measure. Although closely tied to broader efforts to facilitate the deportation of Syrian nationals, the Ministry of Telecommunications has declared its intention to deploy Optical Character Recognition (OCR) technologies to identify forged identification documents and thereby prevent the issuance of SIM cards to individuals without legal residency. Serious concerns have emerged regarding the implementation of this policy, particularly its potential impact on Lebanese citizens through the collection, storage, and protection of personal data associated with OCR use. While the measure appears to align with overarching political strategies aimed at pressuring Syrian refugees to return, it lacks a clear legal foundation and is likely to further aggravate the already vulnerable conditions faced by displaced Syrians residing in Lebanon (SMEX, 2024b).

Ultimately, independent media and journalists are, as of today, the most active groups exposing the corruption of Lebanese élites. Thanks to online and offline transnational networks, they carry out extremely important work in raising awareness about their living conditions under constant threats by the state. Due to the difficulties in identifying a flaw in the legal framework concerning the abuse of cybersecurity by the Lebanese authorities, the most successful strategy for exposing the brutality of online and offline repression is appealing to the respect of freedom of speech. For instance, since 2020, the Coalition for the Freedom of Speech in Lebanon is one of the most active transnational organisations monitoring the actions of Lebanese law enforcement agencies and setting up solidarity networks. Inevitably, the work of independent media and journalists is obstructed by sectarian élites who, thanks to their presence at every critical level of the State's apparatus, attempt to undermine the credibility of investigations in every possible way. A recent example involves the corruption allegations made against the candidates for the presidency of the Central Bank of Lebanon, which paved the way for a government complaint against independent media outlets which investigate on the mismanagement of the 2019 economic crisis (Amnesty International, 2025).

Conclusions

The Lebanese case demonstrates how cyberauthoritarianism can be a powerful tool for adapting online legislation to prevent both the dismantle of a corrupted power system and the democratic advancement. The LNCSS, in fact, makes the collusion between the private sector and political élites visible by stating the public sector's dependence on the private one, implicitly acknowledging the entrepreneurial bourgeoisie's pivotal role in defending consociational stability through the enforcement of cybersurveillance.

Lebanese cyberauthoritarianism allows for a reflection on the evolving relationship between the territoriality of law and the legitimate exercise of State's violence. The analysis of the Lebanese case clearly reveals how the exploitation of *Gewaltmonopol* went far beyond physical and non-physical boundaries, enabling State institutions to establish a specific legal framework that overlaps online and offline spaces and redefines the legitimacy of State's policies. The ambiguous jurisdiction of the Cyber Crime Bureau, in fact, is the concrete example of how cyber borders can be shaped accordingly to political needs through the employment of agencies whose legitimacy is questionable. The inclusion of the Bureau among the bodies responsible for cyber security implied a formal recognition of its activities as pivotal for guaranteeing domestic security. This aspect is particularly controversial, as it legitimised a grey area of intervention due to the Bureau's lack of a clearly defined place within the State's institutional framework. The absence of regulation regarding the activities of the Bureau, together with the vagueness surrounding the definition of cybercrime, then, has become the cornerstone of Lebanese cyberauthoritarianism.

The peculiarity of the Bureau lies in its role as the contact point between private surveillance companies, the ISF, and the government's political leadership, thus being itself the evidence of State corruption in both the physical and the non-physical space. Thanks to the LNCSS, the Bureau assumed the functions of both guarantor and watchdog of the élites' power discourse. The LNCSS, in this sense, eliminated the distinction between the State's legitimate use of force and its illegitimate use of violence by reshaping the narrative on threats to national security (Benjamin, 2014; Deibert, 2015). In order to safeguard their position of power, sectarian élites, embedded within both institutions and private companies, reframed the meaning of security in relation to any possible threat to their privilege. Coercive measures, surveillance and the creation of a legal framework that allows those in power to avoid constitutional accountability for their actions were thus functional in legally framing social change advocates as threats equivalent to terrorism.

The incorporation of online dissent into cybersecurity legislation, along with the systematic prosecution of online activism, made the LNCSS the cyberauthoritarian tool designed to legally suppress all political discourses advocating for social change and the end of corruption. Contesting the actions of sectarian élites thus became framed as a national threat. Since the protection of national interests, defined as the economic interests embedded in the élites' power discourse, is considered a collective responsibility, the government, in collaboration with private sector and academia, must lead surveillance efforts to safeguard these interests. The deliberate absence of a clear definition of domestic security serves to extend *Gewaltmonopol* to encompass any activity suspected of posing an existential threat. This effectively lowers the threshold of tolerance towards any counter discourse against the élites, thus legitimising and broadening the authority of law enforcement agencies to protect power relations. As a direct consequence, the boundaries of security between physical and online space are not existing, resulting in increased targeting of activists, civil society organisations and minorities.

Eventually, the development of the LNCSS, centred on the evolution of activism as the grassroot force capable of undermining the existence of political, economic, and reputational advantages of the élites, highlights the consociational opposition to democratic progress. The juxtaposition between the youngest generations and the Lebanese institutions established in the LNCSS is instrumental in safeguarding the interests of consociational élites. Put differently, anything unrelated to the history of Lebanon post-civil war history is framed as a threat to social peace. This instrumental reversal of the country's history, together with the portrayal of demands for human and civil rights advancement as source of instability, formed the theoretical foundation of the élite's discourse of power. Thus, the introduction of the LNCSS legalised the consociational power discourse by providing specific and efficient tools for silencing criticism against Lebanese institutions through the exploitation of the concept of security.

ORCID

Alessia Tortolini 0000-0002-9154-784X

Funding

The research received no grants from public, commercial or non-profit funding agency.

Acknowledgements

The author wishes to thank the reviewers for their comments.

REFERENCES

Abdel Khalek, M. (2020). *Advocating for the Rights of Sexual Minorities within a Sectarian System*. Doctoral dissertation, Lebanese American University.

Abi Ghanem, N. (2017). "The Right to Privacy or The Right to be Forgotten: Analyzing the Shortcomings of Digital Rights (Laws) in Lebanon". In El Helou, R. (ed.). *Threats to Digital Rights in Lebanon*, 17-25. NDU Press.

Abi Yaghi, M. N., & Yammine, L. (2020). The October 2019 Protests in Lebanon: Between Contention and Reproduction. *Civil Society Knowledge Center,* last accessed 8 December 2025, https://civilsociety-centre.org/paper/october-2019-protests-lebanon-between-contention-and-reproduction

Abrahams, A., & Leber, A. (2021). Electronic Armies or Cyber Knights? The Sources of Pro-Authoritarian Discourse on Middle East Twitter. *International Journal of Communication*, *15*, 1173-1199.

AdVox (Global Voices Advocacy) (2015a). *#HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices*, last accessed 8 December 2025, https://advox.globalvoices.org/2015/07/28/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

AdVox (Global Voices Advocacy) (2015b). *For Arab Human Rights Defenders, Hacking Team Files Confirm Suspicion of State Surveillance*, last accessed 8 December 2925, https://advox.globalvoices.org/2015/07/08/for-arab-human-rights-defenders-hacking-team-files-confirm-suspicions-of-state-surveillance/

AdVox (Global Voices Advocacy) (2020). *In Lebanon, journalists and activists who cover protest face threats*, last accessed 8 December 2025, https://advox.globalvoices.org/2020/02/14/in-lebanon-journalists-and-activists-who-cover-protests-face-threats/

Ahmed, Z. U., & Julian, C. C. (2012). International entrepreneurship in Lebanon. *Global Business Review*, *13*(1), 25-38. https://doi.org/10.1177/097215091101300102

Al-Rawi, A. K. (2014). The Arab Spring and Online Protests in Iraq. *International Journal of Communication*, *8*, 916-942.

Allagui, I., & Kuebler, J. (2011). The Arab Spring and the role of ICTs. *International Journal of Communication*, *5*, 1435-1442.

Amnesty International (2015). *Lebanon: Security forces using excessive force against protestors must be held to account*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/news/2015/08/lebanon-security-forces-using-excessive-force-against-protestors-must-be-held-to-account-2/

Amnesty International (2018a). *Lebanon: Detained activists blackmailed into signing illegal pledges*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/news/2018/07/lebanon-detained-activists-blackmailed-into-signing-illegal-pledges/

Amnesty International (2018b). *Lebanon: The security forces must clarify the circumstances of Ghassan Abdallah's arrest and protect his human rights*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/news/2018/05/lebanon-security-forces-should-clarify-the-reasons-behind-the-arrest-of-ghassan-abdallah/

Amnesty International (2018c). *Lebanon: Crackdown on Beirut Pride an "outrageous attempt to deny human rights of LBGTI people*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/news/2018/05/lebanoncrackdown-on-beirut-pride-an-outrageous-attempt-to-deny-human-rights-of-lgbti-people/

Amnesty International (2019a). *Lebanon: Authorities must immediately end the use of excessive force against peaceful protesters*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/press-release/2019/10/lebanon-authorities-must-immediately-end-the-use-of-excessive-force-against-peaceful-protesters/

Amnesty International (2019b). *Lebanon: Investigate excessive use of force including use of live ammunition to disperse protests*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/press-release/2019/11/lebanon-investigate-excessive-use-of-force-including-use-of-live-ammunition-to-disperse-protests/

Amnesty International (2025). *Lebanon: Authorities must immediately dismiss complaint against independent media outlets*, last accessed 8 December 2025, https://www.amnesty.org/en/latest/news/2025/04/lebanon-authorities-must-immediately-dismiss-complaint-against-independent-media-outlets/

Aouragh, M., & Alexander, A. (2011). The Arab spring. The Egyptian experience: Sense and nonsense of the internet revolution. *International Journal of communication*, *5*, 1344-1358.

Arendt, H. (2017). *The Origins of Totalitarism*. Penguin Books.

Arnous, M. (2018). The robustness of sectarian politics in Lebanon: Reflections on the 2018 elections. *Civil Society Knowledge Centre, Lebanon Support*, last accessed 8 December 2025, http://cskc.daleel-madani.org//paper/robustness-sectarian-politics-lebanon-reflections-2018-elections

Assi, A. (2021). *Lebanon's protest movements of 2015 and 2019: A comparative analysis*. Friedrich-Naumann-Stiftung.

Ben Hassen, T. (2018). Knowledge and innovation in the Lebanese software industry. *Cogent Social Sciences*, 4(1), 1-17. https://doi.org/10.1080/23311886.2018.1509416

Benjamin, W. (2014). *Angelus Novus. Saggi e frammenti*. Einaudi.

Chamas, S. (2023). Lil Watan: queer patriotism in chauvinistic Lebanon. *Sexualities*, *26*(1-2), 230-251. https://doi.org/10.1177/13634607211047523

Clark, J. A., & Salloukh, B. F. (2013). Elite Strategies, Civil Society, and Sectarian Identities in Postwar Lebanon. *International Journal of Middle East Studies*, *45*(4), 731-749, https://doi.org/10.1017/S0020743813000883

Collelo, T. (1989). *Lebanon. A country study*. Federal Research Division, Library of Congress

Conduit, D. (2020). Authoritarian power in space, time and exile. *Political Geography*, *82*, 102239. https://doi.org/10.1016/j.polgeo.2020.102239

Conduit, D. (2024). Digital authoritarianism and the devolution of authoritarian rule: examining Syria's patriotic hackers. *Democratization*, *31*(5), 979-997. https://doi.org/10.1080/13510347.2023.2187781

Daher, S. (2021). Unpacking the dynamics of contentious mobilisations in Lebanon: Between continuity and evolution. *Civil Society Knowledge Centre, Lebanon Support*, last accessed 8 December 2025, https://civilsociety-centre.org/paper/unpacking-dynamics-contentious-mobilisations-lebanon-between-continuity-and-evolution

Deets, S., & Abou Harb, L. (2024). Understanding Cycles of Protest and Elections in Lebanon. *Contemporary Arab Affairs*, *17*(3), 442-466. https://doi.org/10.1163/17550920-bja00047

Deibert, R. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in the Cyberspace*. MIT Press.

Deibert, R. (2015). Authoritarianism goes global: Cyberspace under siege. *Journal of Democracy*, *26*(3), 64-78. https://10.1353/jod.2015.0051

Di Peri, R. (2009). *Il Libano contemporaneo*. Carocci.

Di Peri, R. (2014). Re-defining the balance of power in Lebanon: Sunni and Shiites communities transformations, the regional context and the Arab Uprisings. *Oriente moderno*, *94*(2), 335-356. https://doi.org/10.1163/22138617-12340064

Di Peri, R., & Costantini, I. (2023). Navigating the COVID-19 pandemic in consociational systems: The cases of Lebanon and Iraq. *The International Spectator*, *58*(1), 128-145. https://doi.org/10.1080/03932729.2023.2173913

Dixon, P. (2020). Power-sharing in deeply divided societies: Consociationalism and sectarian authoritarianism. *Studies in Ethnicity and Nationalism*, 20(2), 117–127. https://doi.org/10.1111/sena.12327

Dragu, T., & Lupu, Y. (2021). Digital authoritarianism and the future of human rights. *International Organization*, *75*(4), 991-1017. https://doi.org/10.1017/S0020818320000624

Druzin, B., & Gordon, G. S. (2018). Authoritarianism and the Internet. *Law & Social Inquiry*, *43*(4), 1427-1457. https://doi.org/10.1111/lsi.12301

El-Masri, S. (2023). The influence of clientelism on the Lebanese civil society. *Ethnopolitics*, 1-18. https://doi.org/10.1080/17449057.2023.2226520

Esfandiari, G. (2010). Misreading Tehran: The Twitter Devolution. *Foreign Policy*, June 8, last accessed 8 December 2025, https://foreignpolicy.com/2010/06/08/the-twitter-devolution/

Frangieh, G. (2013). *Bureau of Cybercrimes: An Unorganized Online Censorship*, last accessed 8 December 2025, https://legal-agenda.com/مكتب-مكافحة-الجرائم-المعلوماتية-رقاب/ (Arabic)

Freedom House (2020). *Lebanon. Freedom of the net 2020*, last accessed 8 December 2025, https://freedomhouse.org/country/lebanon/freedom-net/2020

Freedom House (2021). *Lebanon. Freedom of the net 2021*, last accessed 8 December 2025, https://freedomhouse.org/country/lebanon/freedom-net/2021#footnote3_dtiq29e

Freedom House (2023). *Lebanon. Freedom of the net 2023*, last accessed 8 December 2025, https://freedomhouse.org/country/lebanon/freedom-net/2023#footnote1_4szno58

Gaillard, J. (2010). Science and technology in Lebanon: A university-driven activity. *Science, Technology and Society*, *15*(2), 271-307. https://doi.org/10.1177/097172181001500205

Halawi, I. (2020). Consociational power-sharing in the Arab world as counter-revolution. *Studies in Ethnicity and Nationalism*, 20(2), 128–136. https://doi.org/10.1111/sena.12328

Hamzeh, A. (2001). Clientelism, Lebanon: roots and trends. *Middle Eastern Studies*, *37*(3), 167-178. https://doi.org/10.1080/714004405

Hart, H. L. A. (1961). *The concept of the law*. Oxford University Press.

Harvie, C., & Saleh, A. S. (2008). Lebanon's economic reconstruction after the war: A bridge too far? *Journal of Policy Modeling*, *30*(5), 857-872. https://doi.org/10.1016/j.jpolmod.2007.04.004

Human Rights Watch (2018a). *Lebanon: Police Shutter Pride Events*, last accessed 8 December 2025, https://www.hrw.org/news/2018/05/18/lebanon-police-shutter-pride-events

Human Rights Watch (2018b). *Misplaced Trust. Freedom of Speech Under Threat in Lebanon*, last accessed 8 December 2025, https://www.hrw.org/news/2019/02/20/misplaced-trust

IDAL (Investment Development Authority of Lebanon) (2017). *Information technology. Fact book*, last accessed 8 December 2025, http://investinlebanon.gov.lb/fr

Kraidy, M. M. (2016). Trashing the sectarian system? Lebanon's "You Stink" movement and the making of affective publics. *Communication and the Public*, *1*(1), 19-26. https://doi.org/10.1177/205704731561794

Lascoumes, Pierre, & Le Gales, Patrick (2007). 'Introduction: Understanding Public Policy through Its Instruments—From the Nature of Instruments to the Sociology of Public Policy Instrumentation'. *Governance: An International Journal of Policy, Administration, and Institutions*, *20*(1), 1–21. https://doi.org/10.1111/j.1468-0491.2007.00342.x

Levitsky, S., & Way, L. A. (2010). *Competitive Authoritarianism: Hybrid Regimes after the Cold War*. Cambridge University Press.

Lijphart, A. (1969). Consociational democracy. *World politics*, *21*(2), 207-225. https://doi.org/10.2307/2009820

Lijphart, A. (1977). *Democracy in Plural Societies*. Yale University Press.

Lijphart, A. (2002). The Wave of Power-Sharing Democracy. In A. Reynolds (ed.), *The Architecture of Democracy: Constitutional Design, Conflict Management, and Democracy*, 37-54. Oxford Studies in Democratization.

Linz, J. J. (2000). *Totalitarian and Authoritarian Regimes*. Lynne Rienner Publishers

LNCSS (Lebanese National Cyber Security Strategy) (2019), last accessed 8 December 2025, http://www.pcm.gov.lb/Library/Files/LRF/tamim/Strategie_Liban_Cyber_EN_V20_Lg.pdf

Lookout & Electronic Frontier Foundation (2018). *Dark Caracal. Cyber espionage at a Global Scale*, last accessed 8 December 2025, https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Mahmalat, M., & Zoughaib, S. (2022). Breaking the mold? Ministerial rotations, legislative production and political strategies in Lebanon. *Governance*, *35*(4), 1029-1048. https://doi.org/10.1111/gove.12644

Majed, R., & Salman, L. (2019). Lebanon's thawra. *Middle East Report*, 292/293, 6-9.

Mazzola, F. (2023). Community policing in areas of limited statehood: The case of Lebanon. *Mediterranean Politics*, *29*(5), 668–699. https://doi.org/10.1080/13629395.2023.2195545

Muhal (2018). *Youssef Abdullah*, Muhal Observatory for Freedom of Expression, last accessed 8 December 2025, https://muhal.org/en/cases/118

Muhal (2020a). *Saeed Abdullah*, Muhal Observatory for Freedom of Expression, last accessed 8 December 2025, https://muhal.org/en/cases/194

Muhal (2020b). *Leen Tahini*, Muhal Observatory for Freedom of Expression, last accessed 8 December 2025, https://muhal.org/en/cases/193

Muhal (2024). *List of cases*, Muhal Observatory for Freedom of Expression, last accessed 8 December 2025, https://muhal.org/en/cases

Nagle, J. (2018). Beyond ethnic entrenchment and amelioration: An analysis of non-sectarian social movements and Lebanon's consociationalism. *Ethnic and Racial Studies*, *41*(7), 1370-1389. https://doi.org/10.1080/01419870.2017.1287928

Open Democracy (2019). *Lebanon's "October revolution": An end to the civil war?* Last accessed 8 December 2025, https://www.opendemocracy.net/en/north-africa-west-asia/lebanons-october-revolution-end-civil-war/

Pearson, J. S. (2024). Defining digital authoritarianism. *Philosophy & Technology*, *37*(2), 1-19. https://doi.org/10.1007/s13347-024-00754-8

Salamey, I. (2021). *The Government and Politics of Lebanon*. Peter Lang.

Salloukh, B. F. (2020). The Sectarian Image Reversed: The Role of Geopolitics in Hezbollah's Domestic Politics. POMPES Studies, *Sectarianism and International Relations*, 37-41.

Salloukh, B. F., Barakat, R., Al-Habbal, J. S., Khattab, L. W., Mikealian, S. (2015). *The Politics of Sectarianism*. Pluto Press.

Sharp, D. (2023). Lebanon unsettled: The spatialities of the October 2019 uprisings. *LSE Middle East Centre Paper Series*, *75*, 7-26.

SMEX (Social Media Exchange) (2017a). *A Brief History of Personal Data Collection in Lebanon*, last accessed 8 December 2025, https://smex.org/a-brief-history-of-personal-data-collection-in-lebanon/#:~:text=Beyond%20the%20absence%20of%20a,anyone%20in%20the%20country%20—%20from

SMEX (Social Media Exchange) (2017b). *The Case of Blocked Blogger: How the MoT continues to violate free expression in Lebanon*, last accessed 8 December 2025, https://smex.org/the-case-of-the-blocked-blogger-how-the-mot-continues-to-violate-free-expression-in-lebanon/

SMEX (Social Media Exchange) (2018a). *Beirut Based Global Cyber-Espionage Campaign a Threat to Local Freedoms*, last accessed 8 December 2025, https://smex.org/beirut-based-global-cyber-espionage-campaign-a-threat-to-local-freedoms/

SMEX (Social Media Exchange) (2018b). *Security Tips in the Wake of the "Dark Caracal" Report*, last accessed 8 December 2025, https://smex.org/security-tips-in-the-wake-of-the-dark-caracal-report/

SMEX (Social Media Exchange) (2024a). *Digital Rights During the War on Lebanon: November 21, 2024*, last accessed 8 December 2025, https://smex.org/digital-rights-during-the-war-on-lebanon-november-21-2024/

SMEX (Social Media Exchange) (2024b). *Lebanon's telecom ministry to suspend mobile SIMs for "illegal" Syrian refugees*, last accessed 8 December 2025, https://smex.org/lebanons-telecom-ministry-to-suspend-mobile-sims-for-illegal-syrian-refugees/

Tlais, S. (2013). دراسة في النصوص القانونية المنظّمة للعمل الأمني في لبنان (A Study of the Legal Texts Regulating Security Work in Lebanon), last accessed 8 December 2025, https://www.lebarmy.gov.lb/ar/content/دراسة-في-النصوص-القانونية-المنظّمة-للعمل-الأمني-في-لبنان

Toubia, K., Djulancic, L., & Gaier, M. (2019). Government Formation in Lebanon: Key Aspects of Internal Obstacles. Konrad-Adenauer-Stiftung, *1*, 1-12.

Twining, W. (1997). *Law in context: enlarging a discipline*. Oxford University Press.

Twining, W. (2000). *Globalisation and legal theory*. Cambridge University Press.

Twining, W. (2007). General jurisprudence. *University of Miami International & Comparative Law Review*, *15*(1), 1-60.

Twining, W. (2009). *General jurisprudence: understanding law from a global perspective*. Cambridge University Press.

Vértes, S., van der Borgh, C., & Buyse, A. (2021). Negotiating civic space in Lebanon: The potential of non-sectarian movements. *Journal of Civil Society*, *17*(3-4), 256-276. https://doi.org/10.1080/17448689.2021.1994202

Weber, M. (2004). *La scienza come professione. La politica come professione*. Einaudi.

Yee, V., & Saad, H. (2019). To make sense of Lebanon's protests, follow the garbage. *The New York Times*, December 3, 2019, last accessed 8 December 2025, https://www.nytimes.com/2019/12/03/world/middleeast/lebanon-protests-corruption.html