Can Turkey's cybersecurity governance be linked to a specific cyber governance model? An analysis of its 2020-2023 National Cybersecurity Strategy and the subsequent measures and regulations

June 2024

2790079U
22110551
78529191

Presented in partial fulfillment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word count: 22420

Supervisor: Aykut Ozturk

Date of Submission: 26/06/2024

Content

List of Abbreviations

Abbreviations	Definitions
AKP	(In Turkish Adalet ve Kalkınma Partisi) Justice and Development Party
BTK	(In Turkish Bilgi Teknolojileri ve İletişim Kurumu) Information and Communications Technologies Authority
CCDOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CHP	(In Turkish Cumhuriyet Halk Partisi) Republican People's Party
CIRT	Computer Incident Response Team
DNS	Domain Name System
DPL	Data Protection Law
GDPR	General Data Protection Regulation
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technologies
IGF	Internet Governance Forum
ITU	International Telecommunication Union
MHP	(In Turkish Milliyetçi Hareket Partisi) Nationalist Movement Party
MTI	Ministry of Transport and Infrastructure
NCSS	National Cyber Security Strategy
NETmundial	Global Multistakeholder Meeting on the Future of Internet Governance
NIS Directive	Network and Information Systems Directive
NSA	National Security Agency
OTT services	Over-the-top services
PDPL	(In Turkish abbreviated KVKK) Personal Data Protection Law/ Legislation
PKK	(In Turkish Partiya Karkerên Kurdistanê) Kurdistan Workers' Party
R&D	Research and Development
RTÜK	(In Turkish Radyo ve Televizyon Üst Kurulu) Radio and Television Supreme Council
SCO	Shanghai Cooperation Organization

USOM or TR-CERT	(In Turkish *Ulusal Siber Olaylara Müdahale Merkezi*) Computer Emergency Response Team of the Republic of Turkey
WCIT	World Conference on International Communication

Can Turkey's cybersecurity governance be linked to a specific cyber governance model? An analysis of its 2020-2023 National Cybersecurity Strategy and the subsequent measures and regulations

Abstract

The emergence of cyberspace, despite the fact that it brought numerous advantages at all levels, has also represented a source of insecurity, threats and attacks. Therefore and as a result of cyberspace's tricky borderless nature, cyber governance became a crucial but challenging policy area for states. Due to the contested nature of cyber norms, countries have been supporting and embracing different cyber governance approaches, the main ones being the so-called multi-stakeholder model on the one hand, and the multilateral model on the other. It is within this context also characterized by its rising authoritarianism, in which Turkey, after having implemented its first cybersecurity policies and regulations and also developed several national cyber security strategies, started to get nearer to the multilateral approach, prioritizing security and digital sovereignty over freedoms.The relevance of this case relies on the fact that Ankara's position within the cyber governance context has been described as undefined and that it possesses features of both main approaches. The mentioned importance has also been reflected by the need to go beyond West-Non-West dichotomies and the limited presence of academic research and holistic studies around this topic focusing on the period from 2020 onwards. By analyzing Turkey's most recent NCSS spanning from the year 2020 till 2023 as well as its subsequent main regulations and measures, this study aims to understand the nature of Ankara's most recent cyber governance approach and identify how the latter has been evolving within the framework of the main cyber governance models and its strengthened authoritarianism. By doing so, this paper shows how Turkey has finally departed from multi-stakeholderism to a clear multilateral and state-centered approach by the hand of pro-sovereignty, interventionist and authoritarian cybersecurity policies.

Keywords: Turkey, Cyber Governance, Regulations, Digital Sovereignty, Multilateralism, State-centered Approach

Introduction

Due to its asymmetrical and dual-use features, added to the rapid pace of technological change, cyberspace is challenging the traditional interpretation of relevant notions such as security, border, human rights, privacy and sovereignty. Therefore, and mainly due to the existence of insecurity, crime and competing interests within cyberspace, cybersecurity and the governance of the latter has become a fundamental area and practice for states' functioning, stability, economy and also their national security and survival. This is the reason why the latter, despite its challenging nature, started to try to regulate cyberspace (Liaropoulos, 2016 and 2017). However, and due to cyberspace's tricky nature

and the existence of competing interests and different preferences among countries, the latter have not managed to fully establish common and consented norms yet, which has led to the emergence of different cybersecurity governance models (Aslan, 2020, Cheng and yang, 2022a, Cheng and Yang, 2022b, Liaropoulos, 2016).

It is within this context that the Turkish case has emerged as an extremely interesting example. In fact, Turkey has been identified as one of the most successful countries in the area of cybersecurity (Ergöçün, 2021, Halisdemir, 2021, SOCRadar, 2021). Ankara's development of several cybersecurity strategies has not only reflected the country's growing recognition of the importance of protecting its citizens, businesses and critical infrastructure from cyber threats but also its commitment to staying ahead in the field and strengthening its cybersecurity posture (Çifci, 2024). The mentioned dynamics were clearly reflected by Turkey's position and evolution within the so-called Global Cybersecurity Index (GCI), which is a world known composite index developed by the ITU to assess the countries' commitment to cybersecurity, measures five different pillars: legal measures, technical measures, organizational measures, capacity building, and cooperation. According to the former, Ankara was ranked 20th among the 194 studied states in 2018 (the most recently published index till now) (Çifci, 2024, ITU, 2017, 2018 and 2020).

Regarding its cyber governance approach more specifically, Turkey has been said to have features of the two main models: multi-stakeholderism and multilateralism. Related to this, Ankara has increased its support for digital sovereignty (Eldem, 2020 and 2021, Halisdemir, 2021, Karataş, 2020, Örmeci et al., 2022). Additionally and in spite of Turkey's capacity to maintain its relatively stable diplomatic and security relations with Western liberal democracies, Europe and NATO members and its similarities with the latter concerning the governance of cyberspace, the mentioned state has also challenged the multi-stakeholder model so favored by the US and numerous of its allies (Towers, 2014). Indeed and based on countries' voting at the WCIT (World Conference on International Communication) and a set of indicators measuring their respective degree of international cooperation, political system and the nature of their civil society, Morgus and Maurer identified Turkey as a potential "swing state" concerning the

establishment of Internet governance. Due to these several aspects, Turkey has been often depicted as a state lying in a kind of “middle”, not only in broader political terms between the West and the East (mainly related to its autonomous FP and rising authoritarianism), but also within the field of cybersecurity governance and the two main models of cyber governance (Eldem, 2020 and 2021, Erdoğan, 2021, Örmeci, et al., 2022)

As already perfectly explained by Cheng and Yang, there is a great need to go beyond the simplistic West-Non-West dichotomy in the area of cybersecurity governance. This is not only because of the lack of a unified “Western” coherent approach, but also because of the rising level of entanglement between the Global North and Global South (2022). Based on this and taking into account the interesting and to an extent undefined Turkey’s position as well as the limited existing academic research and more holistic studies around it focusing on the period going from 2020 onwards; I identified the need to focus and analyze the Turkish case. This was further reinforced by the fact that Ankara had a relatively recent cybersecurity strategy spanning to the year 2023, which had not been deeply analyzed within the broader national context yet. As a result, this research focuses on the latest 2020-2023 National Cyber Security Strategy (NCSS) and the subsequent main measures and regulations adopted by Ankara till the time of the writing (spring 2024).

The study’s main argument goes against the already mentioned idea of Turkey’s apparent “intermediate position" within the cyber governance area. Thus, I highlight that since the mentioned document’s publication, Ankara has been taking a stronger multilateral, interventionist, pro-sovereignty and authoritarian approach in its cyberspace governance. Concerning the analysis, I firstly carry out a content-based analysis of the whole NCSS official document, in which I specifically focus on the aspects and objectives that are connected to cyber governance. This enables me to have a deeper understanding of Turkey’s most recent NCSS, its “apparent and official intentions” and the document’s relation with the multi-stakeholder and multilateral models. After that and with the aim of identifying what they could reflect concerning the mentioned two models, I analyze the main regulations implemented by Ankara since the NCSS’s publication, that is to say, 2020. By mixing the analysis of a relevant official

document and the country's actual policies (but with a great focus on the latter), this paper attempts to carry out a holistic and deep study to fully capture Turkey's cyber governance approach.

Concerning its contribution, the study offers a deep analysis and understanding of Turkey's most recent cyberspace governance, offering insights going in a different direction from what scholars such as Eldem (2020 and 2021) had pointed out about Turkey's intermediate position between the two main cyber governance models. Thus, while in line with Eldem's identification of Turkey's pro-sovereignty turn and neo-Hobbesian view of cyberspace, this research's findings transcends the view of Ankara's apparent "middle" position between two camps. Indeed, it highlights Turkey's total departure from multi-stakeholderism and its further steps towards the multilateral model and pro-sovereignty, interventionist, authoritarian and state-centered policies. As a secondary contribution, this research has also given certain insights about the correlation between political authoritarianism and the mentioned cyber policies, that is to say, between a country's political context and its cyber governance approach and cybersecurity legislation. Last but not least, the last interesting contribution has been the great similarities that exist between Turkey and the EU concerning their cyber governance approach and how Brussel's pro-sovereignty and interventionist policies have operated as a source of inspiration and influence for the former. This aspect has highlighted the importance of further and holistically studying cases such as the EU (which this study did not have an objective to cover) whose supposed "liberal and democratic nature" has not deprived the latter of adopting the same multilateral, sovereigntist and interventionist policies an authoritarian state like Turkey has implemented. This does not only reflect the need to better understand and analyze how political aspects influence a country's cyber governance approach, but also to study if "formal political aspects" even influence the country's cyber governance approach and if there are major differences in terms of cyberspace governance among countries with divergent political systems The question whether there is any genuine "multi-stakeholder state", especially within the so-called democratic and liberal countries, has been another question that has arisen as a result of the analysis.

Literature Review

Before diving into the dominant cyber governance models as well as the states and organizations whose cyber governance approach possesses similarities with the Turkish one; it is important to first explain cyberspace's main features, what cyber governance is and how the latter and its institutions have been evolving throughout time. The second part, covering the models and the broader international cyber governance landscape, will help us to better understand and contextualize Turkey's cyber governance policies.

Cyberspace's challenging tricky nature

First of all, Cheng and Yang (2022a) and Gourley (2014) put emphasis on the fact that cyberspace is composed of physical and non-physical assets. The latter scholar also clarifies that while the physical assets represent the so-called "cyber domain" which includes any asset that enables us to "utilize"; the latter represents just the "space" (which is non-tangible and non-material) in which users operate and interact (2014). Consequently, cyberspace has also been described as a "unique combination of physical and virtual properties" (Nye, 2014: 1). Influenced by the fact that the mentioned "relatively recent space" challenges geographical limitations; there have also been further conceptualizations regarding cyberspace. On the one hand, it can be seen as a "Global Village" with an extraterritorial realm which facilitates citizens' communication and civil society mobilization. On the other, despite cyberspace representing a short of extension of the physical domain and the real world, its status as an "ungoverned arena" (related with the difficulty to govern it), has been also described as a "Virtual Battlespace", highlighting its dangerous consequences for security and stability (Manjikian, 2010). Although cyberspace does entail a global common infrastructure, its lack of geographical borders and physical space make its consideration of a global commons highly difficult, distancing it from other spaces of that nature such as air, sea and space (Liaropulos, 2016). Additionally, the

incredibly large array of conflicting interests of states concerning aspects such as cybersecurity, values promotion, intelligence and cyber warfare, is also another relevant shaping factor (Aslan, 2020). Therefore, it is no surprise that cyberspace also suffers from insecurity and geopolitical competition. All these mentioned conditions are of course influencing and shaping cybersecurity governance and turning the exercise of state sovereignty challenging (Chen and Yang, 2022).

Regarding these governance and sovereignty challenges that the emergence and the strengthening of cyberspace has brought and continues bringing, it is necessary to mention that although states are perfectly able to control cyber-activities that take place within their borders and the external activities that have an impact on their territory; the application of sovereignty to the non-physical side of cyberspace is more complex. This is related to the fact that there is not a unique nor common approach concerning state sovereignty in cyberspace. The main disagreement among states revolve around the three following questions: whether cyberspace is a global common; the way in which state sovereignty should operate and could be exercised in light of the well known attribution problem; and whether the exercise of sovereignty is something that they would benefit from (Gourley, 2014).

As a result and despite the nowadays critical relevance of international cooperation for global cybersecurity governance as a result of the rise of all kinds of cyber threats; the “geopolitization” of cyberspace has led to more inter-state competition and also normative contestation within international cyber politics. These dynamics have consequently made collective actions at a national and international level more difficult. Added to these challenges caused by the traditional power politics game between countries, states have been also losing power due to the prevalent role of the private sector within this dimension. Consequently and with the aim of protecting, maintaining and exercising their sovereignty, states have been employing the traditional tools at their disposal, so ideas such as data sovereignty, national clouds and load data storages have been gaining popularity. However and despite a fragmentation of cyberspace does not seem likely, there is no doubt that cyberspace governance, which is still under construction, entails major challenges. This has been further reflected by the absence of a single regime for governing cyberspace and regulating its

activities (Chang and Yang, 2022, Chiappetta, 2019, Liaropulos, 2016 and 2017, Nye, 2014).

This “divided” governance that takes place in cyberspace (at least partially), which is “*spread throughout technical standard setting fora, private sector organizations, civil society groups, states and international organizations*” (Liaropoulos, 2017: 33); has been evolving and has also led to the development and adoption of two different main governance models/ approaches. Since the mentioned aspects and challenges (such as the existence of competing interests, the complex institutional landscape, and the existence of different preferences regarding the two dominant cyber governance models) have shaped and are still shaping cybersecurity governance; they and the existing debate around them will now be explained.

Cyber Governance Institutions and their evolution

A relevant aspect that has shaped cyberspace governance are its respective responsible institutions (Aslan, 2020, Chang and Yang, 2022a, Liaropoulos, 2016 and 2017). Regarding the regulatory institutions in cyberspace, state agencies are one of the most relevant ones. Even in cases of self-regulation they always have a say and shape the regulatory context and conditions. However, and as a result of the decentralized and deterritorialized nature of cyberspace as well as the cross-border character of cybercrime, the mentioned agencies often face limitations (Chang and Grabosky, 2017). Apart from these state agencies and as a result of a rise in cybersecurity issues, numerous governmental and non-governmental organizations were created or moved their focus towards cyber governance. Despite the so-called Internet Corporation for Assigned Names and Numbers (also known as ICANN) being one of the main authoritative institutions in the field, there are other bodies such as the International Telecommunications Union (ITU) (specialized United Nations (UN) body and the oldest ICT organization, originally established in 1865); the Internet Governance Forum (IGF) created in 2006; and the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial), founded in 2014 (Aslan, 2020, Chang and Yang, 2022, Liaropoulos, 2016, Weiss and Jankauskas, 2019).

The relevance that transnational organizations such as ICANN possess is influenced by the circumstance that, unlike postal systems or telecommunications, which are mainly governed by ITU; cyberspace does not lie under the scope and responsibility of any specialized agency of the United Nations (so it not governed by ITU neither). ICANN, which represents indeed one of the crucial cyber governance institutions, was created in 1998 by the US government as a not-for-profit, public-benefit organization. It is responsible for the Internet Assigned Numbers Authority (IANA) functions, mainly Internet Protocol (IP) space allocations, the Domain Name System (DNS) management, and root server system management. Additionally, ICANN is also responsible for producing policies related to national sovereignty problems (Aslan, 2020, Chang and Yang, 2022, Liaropoulos, 2016, Weiss and Jankauskas, 2019). A highly relevant aspect whose controversy will be later more deeply explained, was the US government's position to exert influence over the organization through the IANA functions contract between the National Telecommunications and Information Administration (NTIA) and ICANN. However, despite its attempt to retain this control, and the US Department of Commerce’s decision to extend the contract with ICANN for one more year in 2015; Washington finally gave up its control over the organization in October 2016 (Liaropoulos, 2016, Shen, 2016). Since then, ICANN ceased to operate as a US government agency and became an independent nonprofit organization that transferred? its responsibilities to the global multistakeholder community. The former continues to manage the most critical aspects of the Internet with legal status under US law (Aslan, 2020, Weiss and Jankauskas, 2019).

Another non-profit organization created to contribute to the field of cybersecurity governance and policy is the so-called Internet Governance Forum (IGF), created in 2006 by the World Summit of the Information Society (WSIS) and under the responsibility of the UN. Although its objective is to serve as a grassroots discussion forum facilitating the gathering of different stakeholders and the debate on digital policy issues, it is an organization that has no real power or influence (as it does not possess decision making mandate) (Weiss and Jankauskas, 2019).

In relation to the UN's role in this area, since 2001 it has been adopting different resolutions encouraging its member states to adopt effective measures to combat cybercrime. One relevant action was the UN's call on its member states to sign the Budapest Convention, drafted by the Council of Europe. The mentioned Convention represents, indeed, the first international of its kind promoting the harmonization of cyber laws and regulations and establishing cooperation among countries to reduce cybercrime. The former, which is also open to non-member states of the Council of Europe, nowadays includes 69 parties and represents the most widely accepted convention on cybercrime. However, numerous countries from highly populated world regions, such as India, China and Russia, have not signed the mentioned document. The non-universal and, to an extent, the limited scope of the convention undoubtedly minimizes its effectiveness (Chang and Graboski, 2017, Council of Europe, n.d.)

The tension between the multi-stakeholder and multilateral models and the rising relevance of the idea of digital sovereignty

Cyber norms are highly contested among states, and the latter have also supported and embraced divergent cyber governance models. While the multi-stakeholder approach proposed mainly by the US and its allies, and the multilateral one proposed by illiberal states such as China and Russia, represent the two dominant models; there was also a period in which a so-called "distributed governance" emerged as an alternative approach, which, however, quickly disappeared (Aslan, 2020, Cheng and Yang, 2022a, Cheng and Yang, 2022b, Liaropoulos, 2016). Although the so-called "state-centered model" has sometimes been also identified as a further model (Tencent Research Institute, 2021); in this literature review and in line with most of the utilized academic papers (Cheng and Yang, 2022a, Cheng and Yang, 2022b, Liaropoulos, 2016, Pohle and Thiel, 2020, Shen, 2016, Towers, 2014), the former will be considered as a specific version of the multilateral model (which should not lead to a misinterpretation of its rising relevance).

Concerning the multi-stakeholder model, which represents one of the two dominant ones, it is relevant to highlight that it has been considered the dominant

and hegemonic cyber governance approach (Bourdieu, 1977, Carr, 2015, Chen and Yang, 2022, Chenou, 2014, Gramsci, 2001, Liaropoulos, 2016). The mentioned model was introduced by the US and has been supported by the latter and the rest of the West. This model, which has, in theory, inclusiveness, representativeness and diversity as core principles; supports an egalitarian distribution of governing responsibilities among all kinds of stakeholders (Liaropoulos, 2016). Consequently, although the nation-state is the source of authority and regulatory power within a national jurisdiction, other actors can also take part in the regulation and governance of cyberspace. Thus, according to the multi-stakeholder model, state and non-state actors; should be heard on an equal basis and be part of the governance process (Aslan, 2022, Chang and Grabosky, 2017, Liaropoulos, 2016, Machado, 2015). The mentioned stakeholders, which should cooperate with each other, can be divided into three main categories: national governments; commercial/private for-profit or non-profit organizations; and civil society including users and consumers (Chang and Grabosky, 2017, Machado, 2015).

As a result, countries supporting multi-stakeholderism, such as Western countries, have been favoring the already explained multi-stakeholder fora and processes such as the ICANN, IGF and NETmundial (Chang and Grabosky, 2017, Chen and Yang, 2022, Liaropoulos, 2017). The supporters of this model argue that the most effective way to establish norms that are widely accepted and respected by Internet users is to include the latter in the political and legislative process, which would increase institutions' and organizations' legitimacy and authority (Liaropoulos, 2016). Therefore, and although the multi-stakeholder model cannot and does not aim to replace states (as only states may enforce regulations), muti-stakeholderism views state-based governance as non-democratic and even authoritarian. This is connected with the model's expectation of civil society actors, private sector organizations and research centers as actors influencing and institutionalizing cybernorms (Cheng and Yang, 2022a, Liaropoulos, 2016, Machado, 2015).

Regarding the model's advantages and disadvantages and its position in the relevant debate about which model should prevail at an international level, it cannot be denied that the multi-stakeholder approach benefits from inclusiveness

and representation. In addition, the strength of the former is also reflected by the fact that the public sector alone is not always the most suitable actor to govern cyberspace. This is because the state is a highly bureaucratic actor, which is not usually the fastest in adopting new technologies, and may also miss the needed expertise to analyze the latest trends (Machado, 2015).

However, the multi-stakeholder model has also been heavily criticized due to its major flaws. The major criticism towards it, which will later introduce the emergence and the growing support towards the multilateral model and the existing rift between the two, has been the challenge that it poses to traditional sovereignty and the hegemonic control that the US retained in Internet and cyber governance through this approach and institutions such as ICANN. Thus, and despite the latter representing the prototype of the multi-stakeholder governance approach, the institution has mainly been under the control of the US Department of Commerce, which led to insufficient government participation and a dubious legitimacy (Aslan, 2022, Chen and Yang, 2022, Nye, 2014, Shen, 2016, Towers, 2014).

Other criticisms towards multi-stakeholderism have been the lack of decision-making in the IGF and the failed attempt of NETmundial to build a consensus due to great-powers' competing interests. Additionally, by promoting a limited role for governments, the multi-stakeholder approach also suffers from a lack of legitimacy. This is related to the fact that private and civil-society actors, who are given more powers under this model, both lack the necessary institutions and transparent mechanisms to appear as the legitimate regulators in cyberspace (Liaropoulos, 2016 and 2017). Moreover, although civil society is given a relevant role, it does not often possess the organizational capacity or resources from the other sectors, and may also lack relevant and technical expertise (Machado, 2015). Therefore and considering the existing alignment of US national interests with its private sector in terms of Internet and cyberspace governance; there is also an evident unbalanced representation of civil society and private corporations (Liaropouos, 2016 and 2017).

As a result, multi-stakeholderism does not necessarily lead to a more inclusive and global representation of interests (ibid). Consequently, the mentioned

approach has been accused of strengthening the existing power dynamics in favor of the US and its industry (Chen and Yang, 2022) . This has been reflected by Washington's practice of expansion of its sovereignty in cyberspace, highlighted by its legal right to network monitoring on grounds of nationals security needs, its intent to maximize the freedom of cyber operations, its support to the right to freely use "self defense" in cyberspace and the fact that it maintained sovereignty control over the process of handover of IANA's regulatory authority (Shen, 2016). Based on that, multi-stakeholderism has also been depicted as the US discursive tool employed to build an hegemonic discourse with the objective of avoiding the emergence of any kind of challenge to the existing system (Bourdieu, 1977, Carr, 2015, Chenou, 2014, Gramsci, 2001). A system which is controlled, reflects and favors US hegemony and interests (often also the EU), and neoliberalism (Aslan, 2020, Cheng and Yang, 2022a, Cheng and Yang, 2022b, Chenou, 2014, Liaropoulos, 2016, Machado, 2015, Pohle and Thiel, 2020, Shen, 2016).

Consequently, the multi-stakeholder cyberspace governance model started to be challenged by non-Western and emerging-market nations, such as China, Russia, Brasil, India, Indonesia, South Africa, and Turkey among others. Features of this model and the institutional and geopolitical context, as well as specific events such as different incidents of cybercrime, cyber espionage and cyberwarfare; led numerous states, even some allied with Washington, to start asking for some changes (Chang and Yang, 2022b, Kim, 2022, Liaropoulos, 2016, Shen, 2016, Towers, 2014).

The revelations made by Edward Snowden about the incidences of surveillance of international data by the National Security Agency (NSA) (Pohle and Thiel, 2020, Shen, 2016, Towers, 2014) contributed without any doubt to this critical environment characterized by the rising demands to distance Internet and cyberspace governance from the U.S. government (Towers, 2014). Indeed, it also led to a stronger perception by states of the need for digital sovereignty. However, while Western sovereign states, due to their technological superiority, have been and are interested in integrating liberal norms into their policies, and in multilateral institutions and international treaties, and are also (due to their self professed value superiority) attempting to promote these norms to the rest of the

world; non-Western countries are also trying to reflect their own preferences and demanding norms adapted to their cyber governance reality (Cheng and Yang, 2022a). Many of those states, because of their historical experience (often of a colonial nature), are not only very critical of Western countries' hegemony in international bodies, but also give national sovereignty a tremendous importance. Therefore, the former, and especially the current rising powers, have been and are trying to play an active role in the reformulation of norms in cyberspace governance. It is as a result of this context and these dynamics among non-Western, and illiberal and authoritarian countries and also among certain EU member states; that the multilateral cyber governance model started to gain momentum since around 2014 (Cheng and Yang, 2022a, Cheng and Yang, 2022b, Liaropoulos, 2016, Pohle and Thiel, 2020, Shen, 2016, Towers, 2014).

Regarding the features of the multilateral model, in contrast with multi-stakeholderism, it has the defense of state sovereignty as its cornerstone (Aslan, 2022, Liaropoulos, 2016). This is, of course, related to the fact that multilateralism views cyberspace in Hobbesian terms so that the latter, as a result of its insecure and anarchic nature, tends to reflect traditional power structures, competing interests and security dilemmas (Liaropoulos, 2016). Due to the multilateral approach's prioritization of national sovereignty, its proponents support that nation-states should be the only actors putting policy and power exclusively in their hands (Aslan, 2022). Additionally, since this model is a form to coordinate the relations among three or more states based on predetermined rules, this approach supports the creation of relevant bodies within the UN system. However, these multilateral institutions should never prevent states' right and ability to choose their own national cybersecurity policies. That is why multilateralism is in favor of giving non-state actors, such as transnational firms, NGOs, scientists and law experts, an exclusively consultative role (ibid). All these aspects are supported by multilateralism in the name of social order, national sovereignty, and a tighter control of information flows (Aslan, 2022). Therefore and due to its strong defense of the Westphalian notion of sovereignty and the non-interference principle, the multilateral model should follow the same line as the UN body of ITU. This is because the latter empowers its sovereign member

states to choose the organization's policies, limiting at the same time civil society's influence (Aslan, 2022, Chen and Yang, 2022, Liaropoulos, 2017).

Concerning this model's advantages, it is evident that it does not pose any threat to state sovereignty nor presents "legitimacy problems" (at least of this kind). This aspect, which seems also more appropriate and fair concerning the existing inequality in terms of power and resources among world sovereign states, could indeed enable a more equal representation among them. However, multilateralism has clear disadvantages and dangers too, as the reduced and limited role that non-state actors are given could also lead to a certain overrepresentation of states' and ruling governments' interests, harming other non-state actors groups' potential to have different inputs (such as corporations and civil society). Additionally, this great defense that this model makes of sovereignty, could also be instrumentalized by states, ruling elites, governments and political parties to maintain its grip on power, by shutting down for instance political rivals, segments of society, etc. (Belli, 2021).

Coming back to the question of who are the supporters of multilateralism, it is worth noting that the latter has traditionally been supported by non-Western and/or illiberal states such as Russia, China, India, Iran and Saudi Arabia. Other countries such as Turkey, Indonesia and South Africa and developing nations have also challenged multi-stakeholderism (Aslan, 2022, Chen and Yang, 2022, Liaropoulos, 2016 and 2017, Towers, 2014). Due to many developing countries' inability and/or difficulty to keep up with the evolution of information and communication technologies and the major unequal distribution that there is in terms of resources, technology and Internet-related infrastructure among states, they have highlighted how relevant it is for them that their governments exercise sovereignty in cyberspace (Liaropoulos, 2016). As this would help them to avoid destabilizing events such as the fall of governments and insurrections among others. This need and perspective was further strengthened by the dynamics that emerged in the Arab Spring, the Syrian Civil War and the war against ISIS. Therefore, it is not a coincidence that organizations which many of these states belong to and support, such as ITU and the SCO, are clear examples of this multilateral model (Chang and Yang, 2022, Kim, 2022, Liaropoulos, 2016, Shen, 2016, Towers, 2014).

ITU, which is a UN body responsible for international communications and directly challenges the multistakeholder approach, is these states' preferred institution for governing cyberspace. On the other hand, the SCO, an organization which Russia, China, India, Iran and other Central Asian states belong to, is an example of multilateral cooperation between countries that favors a highly controlled Internet. In fact, SCO's member states have not only coordinated their Internet security policies through the mentioned organization, but have also carried out cyber-exercises intended to counter "online" political insurrections. These supportive dynamics towards multilateralism (and its consequent stringent state control of cyberspace) are a further reflection of certain states' interest (mainly non-Western and illiberal) in territorializing cyberspace and thus replacing multi-stakeholderism (Liaropoulos, 2016).

States and organizations of states which like Turkey, have questioned and revisioned the US-centric multi-stakeholderism

Before identifying which states and groups of states share similarities with Ankara's cyber governance approach; it is worth noting that despite the already mentioned trends concerning each state's preference and own approach (considering its domestic and external dimension) and the prevalence of the multistakeholder and multilateral models; there is no clear division of "camps". Thus, there is no real and visible West-Non-West division, as they do not represent homogeneous blocs (Aslan, 2020, Chen and Yang, 2022a and 2022b). On the one hand and although the US and the EU both have embraced multi-stakeholderism, there are major differences concerning their respective cyber governance approach. The existence of divergent positions and approaches also within the "non-Western" camp and the countries that are critical and sometimes directly oppose US cyber governance hegemony and the multi-stakeholder model (encompassing states such as China and Russia, but also the rest of the BRICS and even ASEAN); further reflects the mentioned pattern. Additionally, there are also states which seem to lay in a kind of middle between the two models and sides, such as ASEAN countries; certain BRICS such as India, South Africa and Brazil (Aslan, 2020, Chen and Yang, 2022a and 2022b, Kim, 2022, Rebello, 2017); and the so-called swing states identified by Maurer and Morgus

(2014) (at least some of them) which Turkey is part of and has been identified as lying in this position as well (Eldem, 2020 and 2021, Erdoğan, 2021, Örmeci, et al., 2022). All this also reflects the need to transcend simplistic divisions while analyzing cyber governance models and specific cases.

Due to the differences between all these states (concerning the region they belong to, their political system, culture, etc.), it becomes highly difficult to encompass them in a specific category. This is why I have simply identified the mentioned states as the ones who have mainly questioned and revisioned the hegemonic multi-stakeholder model supported by the US. In the following paragraphs, I will be focusing on the countries and groups of countries which Turkey shares aspects of cyber governance with. By doing so and going case by case, I will be highlighting which are the specific policies Ankara shares with them. In summary, Turkey has similarities with the EU in relation to the idea of digital sovereignty and autonomy and its data protection legislation; with the BRICS the same aspects as with the EU and the their mutual opposition to multi-stakeholderism and to the private sector's influence as well their prioritization of security aspects; with ASEAN member states their intent to couple their defense of non-interference and autonomy with their interest in maintaining good relations with the West and not aligning themselves with a specific block; and with the SCO which China and Russia belong to, its support towards a multilateral and state-centered cyber governance based on cyberspace's territorialization and a highly controlled Internet.

On the one hand and regarding the EU, there is a relevant similarity that Turkey shares with the latter, which is their respective policy directed at protecting data. Indeed and as a result of the EU's intent to achieve digital sovereignty and achieving strategic autonomy in cyberspace (despite being a supporter of mult-stakeholderism); Brussels (in contrast to the US) developed several legislations including a risk management-based regulatory approach, such as in the case of GDPR (Barrinha and Christou, 2022). The so-called GDPR, which is a privacy and security law which was passed by the EU on May 25, 2018, is considered one of the toughest laws of its kind in the world and it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU (GDPR.EU, n.d.). Its adoption which put a greater emphasis on

accountability to the public and data sovereignty counterbalancing corporate interests (especially foreign ones) and that have turned the EU into a regulatory power (Chen and Yang, 2022b, Liaropoulos, 2021); has been a result of a "sovereignist" position and has challenged the predominant US-centric approach within the Western community (Chen and Yang, 2022a and 2022b). The adoption of this legislation has enabled the EU to "create a single market where the subjects are provided with adequate protection concerning their personal data" (Erdoğan, 2021: 227). Similarly, Turkey has been taking steps in terms of personal data protection and privacy rights, as highlighted by the adoption of DPL (which has been based on the EU's GDPR) (ibid).

The BRICS, despite being a collective which is not as homogenous and ideological as it is often portrayed and that has relevant internal discrepancies in relation to Internet governance (Rebello, 2017), do also possess certain features that match with Turkey's cyber governance approach. Although the BRICS, unlike Turkey, have not signed relevant regulations such as the Budapest Convention; they, similarly to the EU and also Turkey, have also been raising the relevance of digital sovereignty. This international trend has thus also been present in these group's members, who have seen the need to control technology as one of their priorities. Therefore, the BRICS have not only invested in increasing their respective digital capabilities, but have also been developing legislations promoting "Internet sovereignty" and data protection (promoting for instance that a person's data should be stored in that person's home country). This has been highlighted by different developments such as India's support of storing Indians' data exclusively within the country and Russia's Sovereign Internet Law and its 2017 update of its data protection legislation (Belli, 2017).

There are also some differences among the mentioned collective, which can als help us to identify further similarities with Turkey's position. Apart from the fact that not all of them possess the same capabilities to shape global governance (Rebello, 2017), Ebert and Maurer divide the collective in two groups: one embracing an "intergovernmental" approach and the other a "sovereigntist" one (2013).

On the one hand, India, Brazil and South Africa, which would belong to the former, want to reposition the central authority of global Internet governance

within multilateral organizations such as the UN and ITU. By doing so, and despite embracing numerous norms part or aligned with the multi-stakeholder model, they ultimately want to limit the role of the private sector (which, as I already mentioned, responds often to Western interests).

On the other hand, Russia's and China's "sovereigntist" approach is much more concerned with territorializing cyberspace, aimed at reducing not only the role of the private sector and companies, but also governments and multilateral institutions (De Gregorio and Radu, 2022, Tencent Research Institute, 2021). This model, which is also known as the "state-centered" one (Kadlecová, 2024, Zhang, 2019), supports the creation of an Internet that aligns with national borders and interests, tends to be highly interventionist and favors national security over civil liberties. Therefore in this approach supported by Beijing and Moscow, the inviolability of state sovereignty in cyberspace is one of the most relevant pillars and the government holds the ultimate authority in the cyber domain (Kadlecová, 2024).

Despite these differences, all BRICS have supported an increased role for the state, a reduction for the private sector, and opposed multi-stakeholderism. This state-centered model added to its logical strong support for sovereignty and the adoption of so-called "security-first" norms in cyberspace (Ebert and Maurer, 2013), have also been adopted by different Arab states. Even countries and organizations of states which are not usually included in the same category of authoritarian states such as the EU, have been, as already mentioned, adopting a strong digital sovereignty stance (De Gregorio and Radu, 2022) (Tabansky, 2021) (Deibert and Pauly, 2019). This approach is indeed also in line with Turkey's recent steps concerning its cybersecurity governance, characterized by Anakra's prioritization of security matters and digital sovereignty and the Turkish state's rising role in cyberspace (Eldem, 2020 and 2021).

ASEAN is another collective whose cyber governance model possesses certain similarities with the Turkish one. While ASEAN states prioritize principles such as non-interference, consensus-based decision-making and regional autonomy; the former have not strongly opposed multi-stakeholderism. Therefore and although this group's support for the respect of state sovereignty could highlight its closeness to perspectives such as the Chinese and the Russian; its expressed

intent to develop a “mutli-disciplinary, modular, measurable multi-stakeholder approach to cybersecurity capacity” reflects this collective’s alternative approach. This has been indeed identified as an attempt by ASEAN to establish a middle way transcending the simplistic West-non-West dichotomy and US’s and China’s respective models (Chen and Yang, 2022b) (Ali, 2021). These dynamics are very similar to the ones in Turkey. While Ankara has maintained its strong diplomatic and security relations with Western liberal democracies (although in decline), its engagement in information sharing and capacity building, its cooperation with other actors like NATO, and even its decision to apply the Budapest convention; the former have also adopted more “statist and interventionist” cybersecurity policies prioritizing digital sovereignty. Thus and despite Turkey’s adoption of certain visions that align with the Russian and Chinese approaches (state-centered and sovereigntist); the former has been depicted as lying within a kind of middle between the two models. This is because while it has not fully abandoned multi-stakeholderism; Turkey has been adopting a more realist and Hobbessian perspective on cyberspace, which has led to an increase of control by the Turkish government over the latter (Eldem, 2020 and 2021). These dynamics also align with the SCO’s cybersecurity approach, which has been characterized by its member states’ preference for a highly controlled Internet. SCO states’ exercise directed at countering online political insurrections have been a further reflection of their support towards a multilateral and sovereigntist model, favoring the territorialization of cyberspace (Liaropoulos, 2016).

As a result, Turkey has been mainly identified as a country lying between the multi-stakeholder and multilateral approaches. However and due to its recent measures, its authoritarian turn and the fact that its relatively close relations with Western and European countries is no proof of its alignment to a specific model; I decided that the former’s latest National Cyber Security Strategy (2020-2023) and the subsequent measures and regulations needed to be studied and analyzed. By revising Turkey’s position within cyber governance and offering a better and deeper understanding of its approach, the aim is to determine the latter and see whether it can be linekd to a specific governance model.

Theoretical framework and methodology

In this part, I will explain the theories that I have used for this study, which are two main cyber governance models: the multilateral and the multi-stakeholder, with the latter also including the state-centered approach. By summarizing their respective main features, I want to offer a brief and comprehensive summary of them (as the models have already been deeper analyzed in the literature review). After that, I will be also explaining how I intend to apply them and which is the methodology adopted by the study.

Before diving into the theories, it is important to highlight (as already mentioned in the introduction) that the objective and motivation behind this study is to fully understand Turkey's cyber governance approach. After its approach had been analyzed and described as one lying between the multi-stakeholder and multilateral models, I wanted to further analyze the Turkish case and study whether this was the case, especially since 2020. This idea and need were not only reinforced by the fact that Ankara has published a NCSS spanning from the year 2020 to 2023, but also by its recent cyber and Internet regulations and their apparent authoritarian realm. The interest and need to focus on this specific case were also strengthened by Turkey's current political context and its progressive authoritarian turn. As a result and with the aim of analyzing Turkey's most recent governance of cyberspace, I came to the conclusion that this topic needed to be analyzed with the help of the theories of cyber governance models. My assumption and hypothesis is that Turkey, considering its political authoritarian turn and the nature of different cyber regulations, could have already departed from a multi-stakeholder approach towards a multilateral one.

Regarding the multi-stakeholder model, which was introduced by the US and has been supported by a large majority of the so-called "Western World", represents the dominant and hegemonic approach of cyber governance (Bourdieu, 1977, Carr, 2015, Chen and Yang, 2022, Chenou, 2014, Gramsci, 2001, Liaropoulos, 2016). Due to this approach's defense of ideas such as inclusiveness,

representativeness, diversity and especially equality among stakeholders; it claims that non-state actors should be treated and heard on an equal basis as state-actors (Aslan, 2022, Chang and Grabosky, 2017, Liaropoulos, 2016, Machado, 2015). Thus, the models highlight the importance of cooperation among national governments, private for-profit or non-profit entities and civil society, the latter including individuals, users and consumers (Chang and Grabosky, 2017, Machado, 2015). This is why by this model, in case of the development of cyber regulations and laws, the mentioned non-state actors should also be consulted and take part in the process. While this cyber governance model has been praised for its inclusiveness and its capacity to integrate different actors's perspectives and demands as well as to help mitigating the slow bureaucratic character of the state (at least potentially) (Machado, 2015); the former has also been criticized due to its potential weakening impact of states' sovereignty. Another strong and fair criticism has also been the control that the US has retained over the Internet through the institutions known as ICANN, institution that despite being based on a multi-stakeholder cooperation, has been controlled by Washington through the US Department of Commerce (Aslan, 2022, Chen and Yang, 2022, Nye, 2014, Shen, 2016, Towers, 2014). This situation did indeed lead to a lack of confidence in the model by several states, which was also reinforced by the unbalanced international distribution of power and the hegemony and weight US institutions and its tech companies did already enjoy.

As a consequence of this context, different states, especially non-Western ones, started to challenge the multi-stakeholder approach and started to develop and support what has been recognized as the multilateral model (especially since 2014) (Cheng and Yang, 2022a, Cheng and Yang, 2022b, Liaropoulos, 2016, Pohle and Thiel, 2020, Shen, 2016, Towers, 2014). This model, which views cyberspace in Hobbesian terms, has the defense of states sovereignty within cyberspace as one of its pillars (Aslan, 2022, Liaropoulos, 2016). Due to this anarchic structure also prevalent in cyberspace and the subsequent importance of national sovereignty, the multilateral model defends that nation-states should be only decision-making actors. This is the reason why multilateralism favors the creation of cyber governance bodies within the UN system, as this framework is

based on respect towards states' sovereignty, independence and autonomy. As a result, while the multilateralist approach does not deny the possibility of non-state actors taking part in cyber governance processes, under this model the latter are only given a strictly consultative role, limiting their impact (Aslan, 2022, Liaropoulos, 2016). While this model does clearly not threaten states' sovereignty, possesses thus this legitimacy and could facilitate a more equal representation among states with different a degree of power; the former has also the danger of overrepresenting states' preferences, ignoring non-state actors' interests and even favor cyber governance authoritarian practices in the name of "state's sovereignty, independence and security".

Concerning the so-called "state-centered model", which has been often considered and treated (as this study has done) as a specific version of the multilateral cyber governance model (Cheng and Yang, 2022a, Cheng and Yang, 2022b, Liaropoulos, 2016, Pohle and Thiel, 2020, Shen, 2016, Towers, 2014); the former represents a short of more radical approach (Kadlecová, 2024, Zhang, 2019). Although the state-centered approach is based on the same idea of sovereignty, it aims to further territorialize cyberspace, supporting not only the limitation of the role of the private sector in the governance of cyberspace, but also of international multilateral institutions (De Gregorio and Radu, 2022, Tencent Research Institute, 2021). Thus, this specific approach which is framed within the multilateral mode and seeks the creation of an Internet that aligns with national borders and interests, is even more interventionist and carries out an even stronger prioritization of national security over civil liberties (Kadlecová, 2024).

In relation to the methodology, I adopt a deductive approach, by which I analyze the Turkish case and its recent cyber governance policies and regulations with the help of the two main theories of cyber governance models. By firstly analyzing the 2020-2023 NCSS official document and focusing on Ankara's official objectives and intentions, I try to identify their respective relationship with the two already mentioned models and their meaning. However, since official documents tend to also have their limitations and their ideas and plans do not always end up being implemented, I additionally focus on Ankara's main cyber regulations from 2020 (the publication year of the NCSS) onwards. By focusing on these

regulations' nature, legal consequences and the context in which they were implemented, I try to contrast the analyzed legislation with the theoretical framework to determine which model could it be aligning with. The final objective, with the help of all the findings, is to find out whether Turkey still has an intermediate position within the governance of cyberspace or whether it has finally turned towards the multilateral model by the hand of pro-sovereignty, highly interventionist and even authoritarian measures in support of a highly controlled cyberspace and a restricted Internet.

Contextualization

Contextualization of Turkey’s cyber governance prior to 2020

In order to contextualize Turkey’s most recent cyber governance and its 2020-2023 NCSS and subsequent regulations, I will be explaining the country’s evolution in this field, focusing on its previous cybersecurity policies, its institutions and legislation. Additionally and since it is another relevant aspect concerning a country’s cyber governance approach, this part will also focus on Ankara’s position within the international cybersecurity arena and its relation with other countries, international organizations and conventions.

First of all, concerning Turkey's general cyber policy, and specifically its strategies, Turkish authorities published two of them that preceded the one analyzed in this study (2020-2023). The “National Cyber Security Strategy and 2013-2014 Action Plan”, which can be considered the country’s first NCSS, entered into force after being published in the Official Gazette as Law No. 28683 June 20 2013 (MTI, 2020). The action plan embedded in this strategy, which included definitions, objectives and principles that needed to be fulfilled in the short term (Örmeci et.l, 2022), had the objective of creating the legislative foundation for the country’s cybersecurity. Thus, it sought to protect national critical infrastructure either run by the public or private sector, the systems used in the services provided by public bodies, and their data, and also to develop cybersecurity technologies and to train human resources (Çifci, 2024). The document also mentioned three principles that needed to be considered in Turkey’s exercise of ensuring its national cybersecurity. On the one hand, cybersecurity needs to be maintained through the use of methods based on risk management and regular improvement. Second, the perspective and approach towards cybersecurity should go beyond the technical dimension, so it should also consider the legal, administrative, political, economic and social dimensions. Last but not least, the risk management approach should be based on strategies focused on removing technical vulnerabilities, avoiding attacks and threats, and reducing potential damages (Örmeci et.l, 2022).

Regarding Turkey's second Cyber Security Strategy, the latter covered the period between 2016 and 2019. The plan embedded in this NCSS was more accessible than the previous one, and its scope, vision and mission were more emphasized (MTI, 2020). One of the strategy's main objectives was to include cybersecurity in national security as well as to develop the needed administrative and technological tools to secure all systems and stakeholders in cyberspace. Concerning the main threats that this strategy identified, they were denial-of-service attacks on public and critical infrastructure, targeted attacks focused on obtaining R&D confidential information and know-how, and hacktivism with political purposes (IISS, 2023). By doing so and with the aim of keeping cyber risks at a manageable and acceptable level, several studies focused on different topics and areas were carried out: strengthening cyber defense, protecting infrastructure, fighting cybercrime, raising awareness and developing human resources, developing cyber security ecosystem, and integrating cyber security into national security (MTI, 2020).

In relation to Turkey's main cyber institutions, the Ministry of Transport and Infrastructure is the main institution responsible for the control and management of cyberspace within Turkey (Örmeci et al., 2022). Thus, it also oversees all other cybersecurity entities throughout the state. Concerning the Ministry's specific functions, it is not only responsible for the implementation, administration and coordination of national cybersecurity actions, and the preparation and coordination of policy, strategy and action plans (Halisdemor, 2021), but it also ensures the establishment of technical infrastructure in public institutions and organizations, carrying out awareness and training activities (Örmeci et al., 2022). Additionally, there is also the Information and Communication Technologies Authority, also known as BTK, which represents other Turkish relevant cybersecurity and cyber governance institutions. Being established as a department under the mentioned Ministry in November 2008, it is the main regulatory institution in cyberspace and the electronic communication sector. As already mentioned and after the coup attempt, the mentioned agency was given all the former responsibilities that held TIB. As a consequence and since then, the BTK is allowed to take any measure in the name of "upholding national

security and public order", "preventing crime", "protecting public health and public morals", or "protecting the rights and freedoms" (Eldem, 2020).

Turkey's domestic Internet policy, which has been evolving, has been characterized by its rising prioritization of control and the defense of its sovereign rights. Concerning one of the first developments related to this, the Turkish state's control of the Internet emerged in 2007 when Ankara started to filter social media content and deny access to specific Internet resources. In order to do so, the state began blocking access to servers, domains, keywords and IP addresses. However, Turkish authorities went further and they did not only pass legislation, but also increased state surveillance, prosecuted Internet users, issued content removal requests and shut websites down (Eldem, 2020).

Turkey's first Internet law was Law No. 5651 entitled "Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publications". It was passed in May 2007. This law, whose approval was justified by the need to protect families and minors, introduced great restrictions and set the criteria for blocking websites. Additionally, the responsibilities of content providers, mass-use providers, and hosting companies and Internet Service Providers (ISPs) were also determined. Law No. 5651, which gave TIB the authority to monitor online context and direct hosting and access providers, introduced several categorical crimes by which a website could be blocked (such as the slandering of Ataturk's legacy). As already mentioned, this legislation led to the blocking of thousands of websites (ibid).

Year 2013 was another relevant date concerning cyber governance and cybersecurity legislation. On the one hand, Turkish authorities started to use existing laws as the Penal Code and Anti-Terror Law to penalize online content. On the other hand, the revolts brought by the Arab Spring as well as the Gezi protest movement in Turkey reinforced the idea of social media's relevance in political and social processes (as Twitter and Youtube had been used for these purposes). Consequently, Turkish law enforcement agencies began to closely monitor the impact of digital technologies on Turkey's political arena and society's mobilization. The case of the supposed infiltration of the Gulen Movement into Turkey's state structure and the release of top-level voice records as well as the elections held in this period showed the Turkish ruling elite the Internet's power

and how critical the control over it could be.Thus, Law No. 6639/29, which was passed in 2015, broadened TIB's powers to block content without a court order and enabled relevant Ministers to immediately request the removal of Internet content and/or blocking of a website (in case the court order is delayed and the content risks public or national security). In relation to the failed coup attempted by FETO in July, 2016, Turkish authorities introduced a state of emergency that lasted to 2018 and adopted 32 decrees which further increased state's surveillance. One of the main consequences was the shutting down of TIB, and BTK's new responsibility of "upholding national security and public order" (among other things) (Eldem 2020).

Moreover, the Turkish parliament, under the majority of the ruling AKP and its ally the Nationalist Movement Party (MHP), passed an amendment in 2018 to Law No. 7103, which is theTurkish radio and television legislation. Apart from the fact that broadcasting services providers (through Internet) were now required to obtain a license from RTUK, the latter was now allowed to demand the removal of content or the retraction of access to the platforms. By doing so, this law gave RTUK great regulatory and monitoring power (Eldem, 2020).

Last but not least, Turkey has had a particular role within the international cyber governance context. On the one hand, Ankara has been depicted as a not very active state concerning international cooperation on cyber matters. Apart from the fact that its engagement has mostly been on a bilateral level, Ankara has not been a major influencer within international cyber debates and has also not been part of groups such as the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace. However, the particularity of Turkey's role and its to an extent ambivalent position has been reflected in its parallel officially expressed alignment with the EU, based on its prioritization of operationalising the existing consensus-based norms for states behavior as well as developing a common understanding of international law's applicability to cyberspace (IISS, 2023). Following the same "Westernist" line, Ankara did also sign the Council of Europe's Cybercrime Convention in 2010, which ratified in 2014. However, despite also signing the Additional Protocol to the Convention on Cybercrime in 2016, Turkey has not ratified it yet. Additionally, the Eurasian country, represented by its domestic company STM, took also part in the

European Commission and European Cyber Security Organisations New Strategic Cyber Security Initiative, a public-private partnership STM is a founding member of that aims to create a joint strategy to counter cyber attacks impacting the public and private sector. In spite of this and as already highlighted, the diversity within Turkey's role within the cyber governance international arena becomes even clearer, when we consider that Ankara (also through the voting of regulations) has domestically favored the expansion of the state's role in internet governance (ibid).

This position, which has been logically accompanied by Turkey's prioritization of data localisation and information control, has also made the former to sometimes side with Russia and China. Moreover, Ankara refused to sign the 2018 Paris Call for Trust and Security in Cyberspace, a France-led initiative that sought to promote existing institutional mechanisms to decrease hacking in cyberspace. The former has also been relatively active in the development of cyber partnerships, which include Albania, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Egypt, Iran, Kosovo, Kyrgyzstan, Macedonia, Montenegro, Morocco, Niger, Republic of Sudan, Senegal, Serbia, Thailand, Tunisia and Ukraine (IISS; 2023).

As a result and while it possesses certain close relations with Euro-Atlantic states concerning cybersecurity and has also promoted international cooperation and certain international cyber norms protecting freedom of expression, Turkey has been also exercising its sovereignty and adopting a statist control over the Internet, favoring restrictive measures and the limitation of freedoms.

Contextualization of Turkey's political transformation and its authoritarian turn under the AKP rule

Concerning this part, since the main goal is to offer a nice and complete but brief picture of Turkey's authoritarian turn, I will be focusing on the main events that led the Eurasian country to become an authoritarian state by the hand of the ruling AKP and Erdogan. By doing so, despite being a deeply interesting topic, I will not be diving into any kind of deep analysis of all the reasons behind the

mentioned political transformation nor the different concepts that have been developed to refer to it.

The case of Turkey has drawn the attention of numerous scholars which have led to the emergence of many enriching studies and even a debate about the type of regime that developed in Turkey as a result of its political transformation. Although there are several terminologies that have been used to refer and describe Turkey's current regime, such as electoral authoritarianism, illiberal democracy, delegative democracy and full authoritarianism among others (Yilmaz & Turner, 2016); there is a general consensus about this shift's weakening effect on Turkish democracy and its authoritarian nature (Akçay, 2021, Akkoyunlu, & Öktem, 2018, Çalışkan, 2018, Erensü & Alemdaroğlu, 2018, Tansel, 2018).

The crisis of the Turkish state started during the presidential elections of 2007, and intensified with the crisis of the accumulation regime. This context was perfectly reflected by the Gezi Park protests that took place throughout Turkey in 2013. On the one hand and concerning the period prior to 2013, it was characterized by the rising tensions between the old Republican and secularist bureaucracy and the emerging political elite represented by the AKP government. On the other hand, the mentioned protests emerged as a reaction to the adoption of neoliberalism as well as the centralization of power and a rising authoritarianism within the country. Although the liberal and left-liberals had previously supported the AKP in its fight against the authoritarian Kemalist state, the former started to oppose Erdogan's party, especially due to its disproportionate use of coercive measures (specifically recurrent against the opposition). Despite the major mobilization power that the Gezi protests showed and the major challenge that they represented for the ruling AKP, the Erdogan-led party (often through violent means) managed to suppress them (Akçay, 2021).

Additionally and despite the cooperation between AKP and the Gülenists to weaken the old Republican "guard", this coalition started to be threatened in 2013 when Gülenist persecutors decided to open court cases against Erdogan's government. However, the AKP responded with a major purge of Gülenists from

the judiciary and security forces (Akçay, 2021, Akkoyunlu & Öktem, 2018). The peak of this struggle was the attempted coup against Erdogan's government on 15 July 2016, which did however not succeed (Akçay, 2021, Akkoyunlu & Öktem, 2018). As a consequence of the failed coup, the government declared a State of Emergency, which led to the 2017 organized constitutional referendum, which was finally approved by the alliance formed by the AKP and the more radical Nationalist Action Party (MHP). As a result of the passing of the amendments which granted the Turkish head of state exceptional legislative and executive powers, Erdogan's popularity was strengthened and its authoritarian rule was also reinforced and legitimized. All these developments led to the great weakening of Turkey's republican, parliamentary and secular tradition (Akçay, 2021, Erensü & Alemdaroğlu, 2018, Yilmaz & Turner, 2019).

This authoritarian turn, apart from including the government's resort to the old method of using anti-terror laws to silence opposition political groups, also included nationalist and Islamist policies and the instrumentalization of Sunni Muslim religious identity. This led to the increase of Turkish society's ontological insecurity, especially felt by non-Muslims minorities such as Turkish jews, Alevis, secular and non-believers (Yilmaz & Turner, 2019).

Finally and regarding one of the last main events that reflected Erdogan's and his party's hegemony, I need to highlight that he, as the candidate from the alliance between the AKP and MHP, won the 2018 presidential election. This served the regime to increase its legitimacy (Akçay, 2021). Last but not least, the 2019 Istanbul elections also included an interesting and relevant development which further showed AKP's dubious practices and Turkey's authoritarian turn. After losing the municipal elections on 31 March 2019, the mentioned party denounced electoral fraud, misconduct and irregularities. The High Election Board's polemic decision to repeat the election, which broke the myth of fair elections, was perceived as another step towards the total weakening of Turkish democracy (Yilmaz & Turner, 2019).

As a result of these changes and this process, a new Turkey was established under the leadership of Erdogan. As already explained, this new authoritarian political regime, apart from being based on a populist and Turkish-Islamic

nationalism, has been characterized by a powerful Presidency and a weak check and balances system and lack of separation of powers.

Analysis

Analysis of Turkey's 2020-2023 NCSS

In this chapter, I will discuss Turkey's 2020-2023 National Cyber Security Strategy and Action Plan. Relying on a close reading of the document, I will carry out the first detailed analysis of the mentioned official document and try to identify patterns that could be linked with the main cyber governance models.

Overview of the document

The National Cyber Security Strategy and Action Plan (2020-2023), which represents Turkey's most recent NCSS, was published in 2020 by the Ministry of Transport and Infrastructure (MTI, 2020). This document, which focuses on the policies that will be applied in the mentioned 4-year long period, has been divided into 8 strategic objectives and topics and aims to increase Turkey's cybersecurity by increasing past achievements. By doing so, the strategy and its implementation represent an attempt to minimize the impact of cyber threats, develop national capacities and create a more secure cyber environment within Turkey. The final objective is to turn the latter into one of the most advanced countries in cybersecurity at the international level (MTI, 2020: 15). Although the document does include a brief explanation within the Realization Approach about the relation between the strategic objectives and the actions that should be taken and also two graphs highlighting which action would cover which strategic objective; the former, similarly to the 2016-2019 NCSS (Çifci, 2024), does not include a publicized Action Plan. This differs from some previous NCSS documents which did include the implementations, organizations, and action plans (Akyeşilmen, 2022). This 2020-2023 unpublished plan includes 40 actions and 75 sub-actions related to the already mentioned 8 strategic objectives.

The first strategic objective (MTI, 2020: 23), which is about protecting critical infrastructure and increasing resilience, mentions that Turkey has already been taking steps towards this objective, especially in relation to the industries of

energy, finance, transport, water management, and critical public services. Therefore and to increase the country's resilience, the activities directed to critical infrastructure will be carried out and performed considering the changing cyber threat and technological landscape, cyber threat vectors, and emerging national needs. The activities studies that will be conducted are the extension of international information security standards' application in the public and private sector; preventing vendor lock-in in critical infrastructures; protecting the country's data, improving sectoral regulations and introducing auditing mechanisms; creating contingency plans; and ensuring a safe technological transformation.

Concerning the second strategic objective, "National Capacity Building" (p.24), the latter highlights the fundamental relevance of having qualified human resources to ensure cyber security. Therefore, Ankara does not only want to increase the expertise level of existing manpower, but also to cultivate qualified workers in this field. While the mentioned objective includes the evaluation of the maturity levels of institutional CERTs and their respective improvement, and the regular organization of cybersecurity exercises at all levels (sectoral and institutional); Turkish institutions will also try to increase the expertise of existing personnel, spread the academic cyber security programs and also offer support to students willing to enter the cybersecurity industry. Additionally and due to the identified need of raising public awareness and protecting children online, this subsection also mentions the objective of including awareness raising activities at all levels, with a specific focus on families, children, students, youth, women, elderly and disabled.

The third strategic objective, which is named "Organic Cyber Security Network" (p. 25), highlights the need to develop advanced-level expertise projects to analyze cyber threats and counter them. In this regard, this part also mentions that the establishment of an organic cyber security network could be extremely useful, as it would develop cooperative efforts between people from different subfields and lead to a great exchange of knowledge. Favoring the diversification and the increase of sources would also help in countering cyber threats, since it would also strengthen the USOM and the institutional CERTs. Moreover, the knowledge exchange between public institutions and private sector concerning

cyber threats and the formation of new connections with stakeholders is also seen as crucially important. One of the goals would be to create a live, active and organic cyber security network at national level which maintains 24/7 interaction with all stakeholders.

The fourth strategic objective (p. 26), which refers to the security of new generation technologies, highlights the relevance (also in economic terms) of maintaining a secure use of the Internet of things, cloud computing and also 5G. This part also highlights the need to determine the use of AI and block chain technologies within cyber security.

Regarding the fifth strategic objective “Fighting against Cybercrime” (p. 26), it emphasized the need to regularly update the fighting methods against the latter. Therefore, conducting preventive, deterrent and efficient studies as well as increasing the national capacity and technological means is of crucial importance. The international dimension is also perceived as a relevant aspect, so that international cooperation and knowledge and information sharing are also prioritized.

The sixth strategic objective (p. 26) is about developing and fostering domestic and national technologies. By increasing the number and prevalence of domestic cyber security solutions, it is not only expected to increase the country’s cyber security, but also to foster the private sector’s development and the country’s economy. Additionally and with the goal of further developing the cyber security ecosystem, this subsection also highlights the importance of strengthening the cooperation between public institutions, academia and the private sector. Thus and related with the first idea, the employment of domestic products, especially for the protection of critical infrastructures, represents clear priority. In relation to cyber security test and certification systems, the strategy envisions the goal to increase the brand value of products and services produced with national resources. Their introduction into global markets via export, would make them more competitive and raise their quality.

In relation to the seventh strategic objective “Integrating Cyber Security into National Security” (p. 27), it clearly emphasizes that cybersecurity is an integral

part of the latter. Therefore, not only should cyber security aspects be borne in mind in high-level national security policies, but cyber defense should also be considered alongside land, air, sea and space security.

Last but not least, the eighth strategic objective (p. 28) focuses on improving international cooperation. The latter is viewed as an activity that can complement and even increase the nationally obtained cyber security achievements. This type of cooperation for cyber policymaking, cyber incident response and fighting against cybercrime that is seen as needed and that is mentioned is framed within bilateral and multilateral models. Within this context, the subsection also highlights the relevance not only of increasing trust in cyberspace in relation to international organizations, but also of implementing joint measures, developing joint strategies, and carrying out cooperation studies. Ankara’s perspective on international cooperation is that the increase of its contribution to international activities and the subsequent identification of best practices internationally in the field of cybersecurity could contribute to strengthen Turkey's position in the latter. That is why and also due to the existing need for improving response capabilities against national and global cyber incidents, the organization of international cyber security exercises and conferences as well as capacity-building activities are also of added importance (and have also been organized by Turkey).

Analysis of the NCSS document within the framework of the main cyber governance models

First of all, it is necessary to highlight that due to the fact that the Action Plan was not published alongside the 2020-2023 NCSS (which contains all the specific 40 actions and 75 sub-actions that would need to be carried out by the responsible Turkish institutions); the analysis of the latter’s document will be brief and its respective contribution rather limited (as it is not possible to analyze the mentioned actions). However, since the 2020-2023 NCSS represents the most updated and important document concerning Turkey’s cyber security and cyber governance, it needs to be analyzed. As already mentioned and since the goal is to determine patterns of Turkey’s official document within the framework of the

already explained cyber governance models, only the aspects that can help me to do so will be covered in this analysis.

On the one hand and concerning one of the main sections, the Realization Approach (section number 10 in the document) clarifies that the implementation of the strategy should not only be based on the already explained 11 principles, but that it should also engage all the required stakeholders. Moreover, it also explains that in relation to the design of the required actions and activities that the NCSS includes to reach the expressed national goals and, also the drafting of the latter; public institutions were not the only actors taking part in the process. The private sector, academia and NGOs were indeed algo engaged. In addition and bit more forward within the Realization Approach section within the "Stakeholders part" (10.3), the NCSS document clearly identifies which are the specific actors that are identified as stakeholders within Turkey's cyberspace: "*Public institutions, private sector institutions and organizations, mainly the ones operating critical infrastructures, universities, non-governmental organizations, research communities, individuals in the country and international stakeholders are among the stakeholders in cyberspace"* (MTI, 2020: 30). This part not only identifies them, but it also clarifies their general contribution. In fact, it is clearly stated that regardless of each stakeholder's specific way (directly or indirectly), all of the ones mentioned should contribute to reach the NCSS objectives: *It is aimed to reach the determined targets by direct or indirect contributions from all the stakeholders*" (ibid).

The emphasis made by the NCSS and the Turkish Ministry on the potential relevant role that the private sector and academia could have is further reflected by the sixth strategic objective which highlights the importance of reinforcing the cooperation between the latter actors and also the public sector (especially regarding the aim of developing the national cyber security ecosystem). Ankara's value and inclusion of the private sector is not only further reflected by the NCSS third strategic objective's (Organic Cyber Security Network) framing of the knowledge exchange between the public and the private sector; but also by the fact that the unpublished 75 sub-actions (at least some of them) have non-public actors such as universities and NGOs as their responsible bodies.

While the information included in this part of the NCSS is not specific enough (especially in relation to each stakeholder's role, function, degree of influence and authority, and status) to relate these aspects to a cyber governance model; there is no doubt that Ankara has an up-to-date and also broad and inclusive view of Turkey's cyber governance's stakeholders. Instead of only focusing on the institutions that have traditionally and still enjoy at least de iure "official political legitimacy" and political power such as the public sector; the NCSS aso includes actors that often lack this official political power but that are also relevant figures in cyberspace and cyber governance, such as the private sector (due to its know-how, technology, capabilities, products and resources), academia/universities (due to its scientific knowledge, ability to research and also form future professionals), and NGOs (which often represent relevant segments of society and group of interests).

Although, as already explained, this aspect would not be enough to directly attribute it to a specific cyber governance model, it could be stated that a state strictly sticking to a "state-centered and "sovereigntist" model would likely not refer to all these diverse stakeholders in such a relatively horizontal way and give the already mentioned non-public actors this "feedback role" concerning the design of the NCSS document. This is clearly reflected in the following phrase: "During the workshop attended by public institutions, private sector, academy and NGOs, feedback from relevant stakeholders were received regarding the required actions and activities to reach national goals within the scope of strategic objectives. The draft document was opened to feedback from relevant institutions and organizations, accordingly revised and finalized" (MTI, 2020: 29). That is why we lack specific insights about the specific nature and the official status of these non-public stakeholders' input and feedback (a strictly consultative contribution or maybe a role with some more influence and authority). This feature present in Turkey's most recent NCSS could be reflecting both models, the multi-stakeholder and multilateral one. As the former would be also compatible with a multilateral model, since despite multilateralists' support of nation-states as the only actors developing and adopting policies, they are okay with giving transnational firms, NGOs, scientists and law experts a consultative role (Liaropoulos, 2016) (Aslan, 2020) (Chang and Yang, 2022).

Furthermore, there is another relevant aspect the NCSS mentions that should be addressed in this brief analysis, which is the topic around international cooperation. The eighth strategic objective focuses indeed on improving international cooperation as it is viewed as an activity that could strengthen Turkey's cyber security by increasing its respective domestic achievements in the field. The cooperation which should be applied for cyber policy making, cyber incident response and the fight against cybercrime is mentioned within the framework of bilateral and multilateral models. By doing so, this specific objective also emphasizes the relevance of trust in international organizations as well as the need to implement joint measures, develop joint strategies and cooperation studies. Regarding the strengthening of Turkey's cyber security, the increase of Anakra's contribution to international cooperation and activities, and the organization of international cyber security exercises, conferences and cyber capacity-building activities do also play a relevant role.

While Ankara's focus and prioritization of enhancing its international cooperation is not enough to attribute it to a specific cyber governance approach, the former's support for bilateral and especially multilateral cooperation for the already explained purposes does indeed point in a specific direction. Considering that pro-multilateralism states support giving the central authority (or at least some big part of it) of cyberspace governance to multilateral organizations like UN and the ITU and favor the cooperation within these frameworks, and that the specific states within this category that embrace a state-centered and "sovereigntist" approach usually seek to limit the role of governments and multilateral institutions (De Gregorio and Radu, 2022, Ebert and Maurer, 2013, Kadlecová, 2024, Rebello, 2017, Tencent Research Institute, 2021); this defense by made by Turkey aligns with the multilateral approach. Therefore and although this aspect represents a certain distance from multistakeholderism, the former is not reflecting any state-centered position, skeptical about multilateral cooperation and organizations (which would be present in the Chinese and Russian cyber governance approaches) (De Gregorio and Radu, 2022, Tencent Research Institute, 2021). This multilateral aspect embraced by Turkey (at least rhetorically and embedded in its NCSS) is indeed accompanied by Ankara's strong prioritization, positive view and even enthusiasm for enhancing international

cyber cooperation, to the extent that it is seen as an important and inherent step to reinforce Turkey's cybersecurity. (MTI, 2020: 28: "[...] *international activities are carried out in order to complement cyber security efforts at national level and boost the achievements obtained by them"*). (ibid: "*For the future periods, it is aimed to strengthen the prominent position of the country in cyber security by the increasing contribution and attendance to international activities in this field, and increase the input provided for the national cyber security efforts by identifying the best practices in the world*").

As a conclusion, although there is an explicit mention of the great array of stakeholders there are in relation to Turkey's cyber governance, they seem to lack at the same time any relevant function, responsibility and influence within this policy area. In fact, it has been their "feedback" contribution in relation to the drafting of the NCSS which seems to have been their most relevant cyber governance function expressed in the document. Additionally and despite the great importance that international cooperation is given alongside the NCSS, the document highlights in a very clear way that the cooperation and its strengthening should follow a multilateral type of engagement. Consequently, I argue that despite all the mentioned limitations that the analysis of an official document such a NCSS can have, the already explained developments within Turkey's 2020-2023 NCSS align more with the multilateral cyber governance model.

Analysis of Turkey's post-2020 cybersecurity measures and regulations

After having analyzed Turkey's 2020-2023 NCSS, this part will focus on the main measures and regulations that Ankara has implemented in the field of cybersecurity since 2020 and till 2024 (at least concerning the period when this study is being carried out. As already mentioned in the previous parts, since analyzing the implementation of the NCSS is not feasible especially due to the Turkish Ministry's decision of not publishing the Action Plan, and the fact that the important aspect is not the strategy's degree of implementation itself but the adopted measures; the analysis will exclusively focus on the latter. As a result, there will be no reference to the NCSS's degree of implementation, since only the passed regulations will be the ones guiding us towards the understanding and identification of the main features. This will help us to shed light into Turkey's cyber governance approach and model.

Concerning its structure, the analysis will be divided into four main areas/topics that I have identified regarding Turkey's cyberspace governance since 2020. They are the following: Turkey's relationship with the EU, NATO and the West; non-state actors' lack of role within Turkey's cyberspace governance; the evolution of its data protection legislation; the two interconnected laws known as the "Social Media Law" and "Civil Society Law", and the lastly "Disinformation Law". By focusing on these areas, I show how Turkey has recently been moving further towards a multilateral approach, characterized by its fierce defense of digital sovereignty, the lack of influence of non-state actors within its cyber governance, and its support towards a highly state-controlled Internet. By doing so and by highlighting how Ankara's cyber governance approach lacks features that would align with multi-stakeholderism, I conclude that Turkey's position is quite defined within the mentioned camp and that it does not lie by no means in an intermediate position between the two main cyber governance models. In addition and in relation to the last three laws, Ankara has further moved within multilateralism to the even more interventionist and authoritarian camp of the state-centered approach. Additionally, this part does also highlight the great similarities between Turkey and the EU and how in the Turkish case, several

relevant legislations seem to possess a certain political realm and purpose and have been passed in a particular political context dominated by AKP's and Erdogan's authoritarianism.

Turkey's relationship with the EU, NATO and the West as a representation for its coherent and apparently pragmatic behavior

A country's relations with other states, groups of states and treaties, despite being an external dimension, is an important aspect of its respective cyber governance approach. In this section, I focus on Turkey's relationship with Western countries, specifically with NATO and the EU. The aim is to show that despite Ankara's relatively close relations with the mentioned organizations, this does not mean that the former has somehow adapted its cyber governance approach to the multi-stakeholder model. Indeed, I try to show how Turkey's external relations in this case with these Western actors do not reflect any major shift. Contrary to what it could be superficially perceived, Ankara's position can be best understood through the lenses of pragmatism and geopolitical interests as well as policy coherence. Indeed and especially Turkey's similarities with the EU reflect their convergence concerning the support of their respective digital sovereignty and interventionist policies.

On the one hand, despite Turkey being an official party to the Council of Europe "Budapest" Convention on cybercrime (mainly supported by all Western countries and also states relatively aligned with the West) (Council of Europe, n.d.); it has not signed the Convention's Second Additional Protocol on enhanced cooperation and disclosure of electronic evidence yet, which was already open for signature in May 2022 (European Commission, 2022). In addition, Ankara still has certain declarations and reservations regarding the following Articles of the Convention: 2, 7, 14/ 3 (b), 22,24/7 (a), 27/2 (c), 29/4th para., 35/1, 40 and 42 (Council of Europe, n.d.). In relation with Turkey's role within the framework of the Convention, the former has been quite active in cooperating with other parties, either formally and/or informally assisting them or requesting them assistance and information. An evident example of this was Ankara's behavior when it received a screenshot of a conversation between two terrorist members

of the Kurdistan Workers' Party (PKK) from a source showing their presence in the French capital and their willingness to explode a bomb in Schiphol Airport. Before the terrorist attack could be executed, Turkey informed Dutch authorities, which were then able to take the necessary precautions (Cybercrime Convention Committee, 2020). Moreover, in relation to the cooperation model known as the "24/7 network" that is part of the Convention, Turkey has not only used it to request information, but has also been subject to numerous requests by other parties. Indeed and although we do not have the specific data for 2020, in the last four years since the latter (including it), Ankara successfully responded to around half of the received requests (21/43). Five of them were still in progress in 2020 and the rest could not be delivered due to the unavailability of data or technical problems. Lastly, the Convention also promotes the cooperation between the parties and the private sector (Cybercrime Convention Committee, 2020).

Furthermore and despite its still existent connection with the West, Turkey was not invited to sign a declaration on the future Internet proposed by the EU, the USA and allied states. The reason behind this decision was Anakra's non fulfillment of the criteria "for a trusted Internet which reinforces core democratic principles, fundamental freedoms and human rights" (European Commission, 2022: 38).

In relation to the EU and as a result of Ankara's perspective of the NIS Directive as a relevant regulation, Turkey has been monitoring any legal development of the EU acquis. However, despite its published intention to adopt NIS provisions into Turkish Law, Ankara has not expressed whether its plan and intention have changed as a consequence of the entry into force of the "NIS 2" Directive in the EU last January (Chambers and Partners, 2023). Last but not least and in relation to personal data protection and privacy rights, Turkey has been also taking steps in this realm, as highlighted by the adoption of DPL (which has been based on the EU's GDPR) (Erdoğan, 2021).

Regarding another relevant aspect of Turkey's connection with the West in relation to cybersecurity, Turkey took part in all the NATO Locked Shield Exercises since the publication of its NCSS (including 2024 but with the exception of 2020, as the exercise was canceled due to the pandemic) which is an annual

real-time network defence exercise known by its challenging nature and organized by NATO Cooperative Cyber Defence Centre of Excellence (CCDOE) member states and NATO Partnership for Peace Program member countries. This is an exercise which is aimed to offer cyber defenders the opportunity to practice the protection of national IT systems and critical infrastructure facing a serious cyberattack. Additionally, the former also enables the participating teams (which often have a multinational composition) to put tactical and strategic decision making and cooperation into practice, while also facing and responding to forensic and legal issues (TurDef Global Defence News, 2022) (CCDCOE, 2023).

Concerning the analysis and meaning of these dynamics and events, it is important to mention that Turkey's proactive involvement in the Budapest Convention activities are of relevance. The fact that the mentioned convention signed by Ankara offers a legal basis for international cooperation on cybercrime and electronic evidence and that its parties as members of the Cybercrime Convention Committee take part in the further development of the convention while also exchanging experience and information between each other (Cybercrime Convention Committee, 2020); clearly highlights Turkey's openness, willingness, interest and capacity to actively participate in multilateral settings. In addition, it should also be noted that the clear majority of the Budapest Convention's parties are Western countries, which further reflects Ankara's relatively close and good ties with them, at least within this cybersecurity realm. This is also an important aspect, as the mentioned states are mainly characterized by their support of multi-stakeholderism and also multilateral and international treaties (Liaropoulos, 2016) (Cheng and Yang, 2022a) (Machado, 2015). Although NATO (despite its efforts and information campaigns) cannot be considered an ideological alliance holder of certain values; Turkey's full involvement in its Locked Shield Exercises is another example of Ankara's close relationship with the "Western World".

Moreover, the EU's, the US and other allied states' decision to not invite Turkey to sign the already mentioned declaration on the future Internet shows at the same time that despite Ankara's relative closeness to them, its distance to certain democratic and liberal principles does also create a certain distance and

incompatibility between Turkey and the former. However, Ankara's initially expressed intent to adopt the EU's NIS provisions into Turkish Law and the shaping role that the EU's GDPR has had on the Turkish equivalent PDPL not only shows Turkey's willingness to follow a similar path to the EU and openness to being influenced by the latter, but also its embracement of the idea of digital sovereignty (idea opposed to multi-stakeholderism and neoliberal positions and closely connected with the multilateral and sovereigntist cyber governance approaches).

Last but not least, it is relevant to note that the Budapest Convention enables its parties to improve their cooperation with the private sector, pushing companies to work together with the former's criminal authorities. While this does not mean that the private sector plays a role in cybersecurity governance within the Budapest Convention's parties' respective cyberspace, it shows the latter's and specifically Turkey's acknowledgment of the relevance of the private sector's engagement in multilateral cybersecurity cooperation and in general cyberspace protection. Thus, while it does not directly represent a feature belonging to the multi-stakeholder approach, it represents a clear wink towards the importance that the private sector has within the field.

Concerning these dynamics' deeper meaning, I argue that despite these connections and similarities that Turkey has with the West within certain cybersecurity policy areas, this does not mean that Ankara has moved nearer to certain Western values nor to the cybersecurity model and principles that have been traditionally stronger among Western countries: mutli-stakeholderism. This prevalent relatively close relationship that Turkey still maintains with Western countries as well as its selective adoption of certain or similar policies of the latter does not mean any "pro-multi stakeholder and liberal" turn; but a pragmatic behavior. Indeed, while the Budapest Convention is a clear example of multilateral cooperation that benefits all its parties in their fights against cybercrime, such as the case of Turkey, the former, parallelly, does not force Ankara to adopt any "innovative policy" nor to make any substantial change concerning its cybersecurity governance. More specifically, the Budapest Conventions's framework, due to its multilateral nature, does not require the implementation of any "pro-multi stakeholder" policy that could go strongly

against the idea of sovereignty (which seems to be one of the pillars within Turkey's approach).

In addition, the kind of parties that have signed the Budapest Convention does also reflect a certain "comfort zone" for Turkey, as they are countries which Ankara already have relatively close relations with (despite certain existing tensions or disagreements). Additionally, this relationship with several of these countries has been partially built through Turkey's NATO membership as well as its former "European" aspirations and its contact with the EU. Finally and as it will be later explained, Ankara's decision to adopt a data protection legislation largely based on the EU's GDPR also represents this pragmatic but at the same time selective and coherent conduct. In this sense, Turkey has adopted a EU-styled-policy that aligns with its perspectives and "cybersecurity needs" and that also benefits in this case its economic interests (as we should not forget that in order to carry out business activities in Europe or with European customers, all companies need to comply with GDPR). Since the GDPR is based on the idea of supporting digital sovereignty, Turkey's adoption of a similar law represents a coherent "ideological and doctrinal" move, as it is this idea of sovereignty which has been gaining ground within Turkey's cyber governance approach. Thus, instead of a "European", liberal and pro-multi stakeholder move by Ankara, these dynamics show that the EU's and Turkey's policies have converged when the latter have been based on the same idea (digital sovereignty) and when they have included this statist and interventionist character.

Non-state actors's lack of role within Turkey's cyberspace governance as a relevant "multilateral" feature

Another important aspect in analyzing a country's cyber governance approach is the role of non-state actors. Despite certain references to multi-stakeholderism within Turkey's 2020-2023 NCSS, in this chapter I show how the engagement of non-state actors within the country's cyber governance has been non-existent. Therefore and despite non-state actors' active role such as private companies in training and educational activities, the former have not played any role nor have

any voice regarding Turkey's cybersecurity policy and regulation. In addition and despite certain authors' classification of Turkey as a state with features belonging to the multi-stakeholder model, these analyzed developments further show how Turkey does indeed lack what it represents as a fundamental feature within the mentioned approach. This seems another reflection of Turkey's turn towards a multilateral approach, in which non-state actors lack any kind of relevant leverage.

Concerning the Turkish case, although there is no legal obligation for the private sector to cooperate with the public sector, Ankara has been emphasizing the relevance of working together with both sectors and the mutual trust between them. However, the focus on the private sector's potential contributions has not been so much focused on the governance and regulation of cyberspace (such as the development of measures and legislation), but on the economic side of cybersecurity. This includes objectives such as the strengthening of buyer-supplier relationships, common distribution channels, common networking opportunities, and R&D activities. Therefore, the main idea is to take advantage of the existence of common interests between the public and private sector, specifically between universities and companies, so that the latter, also through their membership in Turkey's Cyber Security Cluster, can become more competitive that the ones operating alone and lead to more general benefits (ISPI, n.d.).

In addition, this limited role of non-state actors within the country's governance of cyberspace has also been reflected by the fact that despite the three last NCSSs (also including the one analyzed here) emphasize on the need for public-private entities to cooperate in countering cyber threats, in practice this cooperation has not been present. A reflection of this is the lack of representatives from non-state entities among Turkey's Cybersecurity Board members and the national regulatory and supervisory institutions. This lack of private participation is also present in public and sectoral CIRT teams (Akyeşilmen, 2022).

There is another reflection of the private sector's lack of voice within the country's cyber governance which is its almost exclusive engagement in educational cybersecurity activities (thus not in governance per se). For instance, there are

cyber security vocational schools organized as a result of the cooperation protocol signed by Turkey's Digital Transformation Office and the Council of Higher Education which will be partially guided by the private cyber security sector. By following this line, pilot schools will be located in technoparks where cyber security companies are usually located. As a further reflection of the relevant role that the private sector will play in this launched educational initiative, experts coming from the latter will be teaching courses and the curriculum will be designed based on the mentioned sector's needs. Additionally, there is also a plan to create a sustainable programme through cooperation models between the private sector and universities (Presidency of the Republic of Turkey, Digital Transformation Office, n.d.).

As a result, these developments and measures mentioned reflect that non-state actors have only been allowed to act in cyber security areas that are not connected to cyber governance. An example of this is that despite cooperation between the public and private sector has been highlighted and companies are involved for instance in delivering vocational schools, they have lacked any representation position within relevant cybersecurity state institutions as well as any real influence in decision-making processes and the design of cyberspace-related measures. As a result, I argue that this shows the alignment of Turkey's cyber governance approach (at least concerning this specific aspect) with the multilateral governance model.

The evolution of Turkey's data protection legislation and its further step towards the EU's pro-sovereignty interventionist approach

Data protection is a governance and legislative measure that is of critical importance not only in Turkey's cybersecurity governance but also within the international cybersecurity context. Therefore and also due the introduction of certain amendments, the Turkish law's recent transformation and evolution in this area will be analyzed. By doing so and also focusing on the Turkish legislation's similarities with the EU, I show how Turkey has used the EU as a source of inspiration for its data protection laws. However and instead of what some would expect, Ankara's rapprochement with Brussle's legislation has been based on

their shared support of protecting and increasing their respective digital sovereignty. This and since the multilateral model is largely based on the idea of sovereignty, this Turkish data protection regulation is another reflection of Ankara's alignment with the mentioned model.

On the one hand, we can observe the first sign of Turkey's PDPL's evolution in 2020, when several policy documents such as the Human Rights Action Plan and the Medium Term Program were adopted. These changes, which were a result of the business sector's demands as well as the rising use of cloud computing software and the emerging challenging need of processing new kinds of data, brought Ankara's approach closer with the EU's GDPR (Güven Tastan, 2024).

Moreover, the year 2021 marked a significant change in this regard, as Turkey's Ministry of Justice formed a Science Committee responsible for drafting new data protection legislation (European Commission, 2022) (Güven Tastan, 2024). The mentioned committee prepared two different legislative packages. The first one, which was published 12 March of the same year, covers the processing of special categories of personal data, data transfers abroad and the competent court for monetary fines imposed by the country's DPA (Data Protection Authority) (Kişisel Verileri Koruma Kurumu). Concerning the second package, which is still in progress and has not been published yet, it aims to fully align the PDPL with the GDPR (Güven Tastan, 2024).

Concerning the transfer of data abroad, the initial version of the PDPL was mainly based on the need for explicit consent for sending data outside Turkey. This method however tended to present issues of revocability and there was also a relative difficulty to obtain the consent. The mentioned amendment's version enabled transfers without consent only via two ways: Either in case of an adequacy decision proving that the foreign country had adequate data protection, or via DPA-approved contractual clauses. The problem with this regulation relied on the fact that not only had the Turkish DPA not identified any state with an "adequate" legislation, but that it had also refused most of the applications. Therefore and due to this need of an update, the PDPL was revised, leading to a major change in the way personal data international transfers are managed (Güven Tastan, 2024). While the old version was based on a consent-based

model, the new started to rely on a structured approach composed by the following tiers: adequacy decisions, appropriate safeguards and occasional cases. As a result, while an adequacy decision by Turkey's DPA is generally needed for transferring data abroad, in its absence, "appropriate safeguards" such as binding corporate rules may apply. In the specific case of absence of an adequacy decision and appropriate safeguards, there are exceptional cases which may enable data transfers. Concerning the case of adequacy decisions, which could apply to international organizations and specific sectors, despite the Turkish DPA has not made any yet, there is the possibility of Ankara negotiating this kind of decision with the EU (ibid).

Additionally, there are also some relevant differences between Turkey's and the EU's data and privacy protection legislation, such as the one present in their respective legal structure reflected by Turkey's DPA's different composition. Indeed, the latter, unlike in the EU, is not autonomous, so its respective members are selected by the Turkish executive power (Franceschini and Falduti, 2023).

As a result of these dynamics there is no doubt that Turkey's recent update of its PDPL data has not only offered a more practical approach and further specified and broadened the cases under which personal data can be transferred abroad, but have also moved Ankara closer to the EU's approach and to the GDPR's standards. Therefore, this has been another example of Turkey's implementation of EU's legal structures (Güven Tatan, 2024) (Franceschini and Falduti, 2023).

As previously explained, this is of particular importance for analyzing and understanding Turkey's cyber governance approach, as the main reason and idea behind the EU's GDPR has been Brussel's objective of forging its "digital sovereignty" and enhancing European autonomy in the digital realm (European Parliamentary Research Service, 2020). Concerning the implications of the GDPR, the latter requires organizations (regardless of where they are based in or they conduct business) to follow and to comply with strict data management rules when dealing with EU customers and users (Broeders et al., 2023). Therefore and due to the GDPR's highly interventionist nature as well as its strong connection with the idea of digital sovereignty and autonomy, Ankara's move towards this direction with its updated PDPL does not reflect a move

towards multi-stakeholderism or liberal positions, but a statist, interventionist, state-centric and sovereigntist policy. As already mentioned in the literature review, this kind of position has been adopted by states' supporters of all kinds of ideologies (as these two cases show) (De Gregorio and Radu, 2022) (Tabansky, 2021) (Deibert and Pauly, 2019) and has challenged predominant US-centric digital and cyber governance approach (Chen and Yang, 2022a) (Chen and Yang, 2022b).

In addition and as already mentioned in the part covering Turkey's relations with states, Ankara's adoption of a GDPR-styled law could also be based on economic considerations. This could be explained by the important trade relations there are between Turkey and the EU and the relevance of GDPR-compliance to any actor (in this case Turkish companies) doing business in the EU and/or offering services/products to people established in EU's territory. Additionally and concerning this same idea but within its domestic dimension, an interventionist and sovereigntist regulation such as the PDPL does also align perfectly with the idea of preserving Turkey's autonomy and sovereignty, since it could also serve to strengthen the Turkish state's control of the country's internal market and foreign companies' activities in Turkey. The Turkish law, as it has been with the GDPR and American companies, could also reinforce the Turkish states' position vis-à-vis foreign actors and companies, thus strengthening again the prevalence of the state over any actor and also the idea of autonomy and non-interference. Last but not least, the harder the compliance of a law, the more this could benefit the domestic companies of the country, in this case Turkey (as many would be already used and prepared for complying with it).

These steps taken by Turkey are another proof of its selectiveness and also "governance coherence" concerning its adoption of EU-similar legislation. This is reflected by the fact that it is the idea of defending Turkey's sovereignty and autonomy (even beyond cyberspace as it has been highlighted by the potential economic reasons behind the law) which seems to be the guiding principles behind the measure and which matches with the latter's nature. This behavior adopted by Turkey does not only perfectly match with the identified by Eldem (2020 and 2021), based on the prioritization of digital sovereignty and an

increased state's role in cyberspace, but it highlights Ankara's alignment towards the multilateral cyber governance model.

The "Social Media Law" and "Civil Society Law" as a reflection of the rising Turkish state's control in cyberspace

Concerning one of Turkey's major regulations in relation to cyberspace, the Turkish government passed in the summer of 2020 an amendment to Law No. 5651, which is the Law on Regulation of Publication on the Internet Suppression of Crimes Committed by Means of Such Publication and has been also known as the "Social Media or Internet Law". This change was indeed introduced through the amendment of the Law No. 7253, which is the Law on Regulations of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications also known as the "Civil Society Law", which was published in the Official Gazette dated 31 July 2020 (APC and Sida, 2022) (Erdem & Erdem, 2020). By analyzing it, I show how the Turkish state has increased its control of cyberspace and specifically social media, which has been enforced in the authoritarian political context that the country experiences. Therefore it is no surprise that mentioned laws have been characterized by an interventionist and authoritarian character, aligning themselves with the multilateral and state-centered approaches.

This "Social Media Law", which included changes that had already been proposed in April 2020 during the first months of the pandemic, finally entered into force after its publication in the Official Gazette (Resmi Gazete) dated July 31, 2020 (APC and Sida, 2022) (Örmeci et al., 2022) (Timucin, 2021). This was a further reflection of the rising level of censorship and persecution by the Turkish state over online users and platforms (Timucin, 2021). Specifically, this measure allowed several things such as mass surveillance of Internet users in Turkey, the introduction of sanctions against social media companies operating in Turkey unless they have complied with the government's orders. The mentioned law also included the removal of content seen as undesirable by government officials (APC and Sida, 2022).

Concerning the amendments introduced by Law No. 7253 to the previous “Social Media Law (No. 5651), one of the most important introduced changes was the one reflected by the supplementation of Article 4, which specifically concerns social media companies with over one million users per day (Timucin, 2021) (Balamir Coskun, 2021). From October 2020 onwards, the international firms falling within the mentioned category, have to appoint a permanent representative with an office in Turkey. This figure is expected to act as the contact person for the responsible Turkish authority. In case of non-compliance, the Information and Communication Technologies Authority (BTK in Turkish) has the right to impose financial penalties which could be also escalated. If a given company would still refuse to register, the mentioned authority can ask the court to slow the bandwidth of the sites to restrict users' access. In case of international companies complying with this article and opening offices within the country, the former are expected to answer to the BTK’s requests and also individuals to block or remove offensive content hosted on their platforms within 2 days. If the company rejects the request, the former has to explain why it reached this decision. In this case, firms are also expected to carry out biannual reports on the implementation of content removal/access blocking decisions. Additionally**,** Paragraph 5 of Article 4, which covers the topic of data storage, is also of particular importance. The former imposes social network providers, independently if they are domestic or foreign, to store data inside Turkey, as this makes it easier for the responsible Turkish authorities to confiscate data about users from tech companies. Last but not least and according to Paragraph 8, if there would be a court decision to remove or block content, all social media companies would be expected to act in accordance with the former within one day of notification. In case of not acting accordingly, companies are liable for the indemnification of any damages (Balamir Coskun, 2021).

Concerning this amendment’s application, the BTK issued in 2020 all concerned foreign-based social media companies that did not comply with Article 4 an administrative fine that ascended to ten million Turkish lira. In addition to that, Turkey’s Official Gazette published in January 2021 the BTK’s decision against Pinterest, Twitter and Periscope. Due to the fact that these companies had not opened a compliance office in Turkey, the BKT banned advertising on the former. This was an effective way to influence social media platforms’ behavior, as such

a ban would make them lose their advertisement revenues. Therefore and despite certain initial oppositions, all social network providers finally complied with the New Internet Law (ibid).

Before diving into the analysis and interpretation of these two relevant amendments, it is also important to focus on the political and regulatory context in which the former was passed. Indeed, a feature of this period was the Turkish government's rising attack on the freedom of press, reflected by the fact that different conglomerates related to the government were already in control of more than ninety percent of the country's conventional media. This is the reason why social media represented such a relevant space, as it appeared to be one of the few spaces for alternative and/or independent information. Thus, it is nor surprise that social media platforms such as Youtube and Twitter had become the means for independent journalists (independent from the government at least) to reach their respective audiences while avoiding at the same time state control (Balamir Coskun, 2021).

In relation to how the government justified these implemented measures, the former highlighted its intent to fight cyberbullying, disinformation, and terrorist propaganda (Balamir Coskun, 2021). Additionally, the Turkish government also specifically referred to the proliferation of fake news in social media. In 2020, Erdoğan did not only accuse social media companies of "digital dictatorship" and "cyberbullying", but it also stated that these platforms were not serving Turkey's interests. By doing so, he did not doubt in expressing that they wanted to shut down the former through the passing of a bill (Reuters, 2020). Last but not least, Erdogan's government also made use of an "external legitimizing aspect" by emphasizing that their just discussed and passed law was based on Germany's Network Enforcement Act also known as "NetzDG" (DW, 2020).

Regarding the analysis and meaning of these amendments, there is no doubt that they represent a further step in the restriction of the media in Turkey. Although the government tried to justify them with the excuse of fighting cyberbullying, disinformation and terrorist propaganda, it is also a fact that the shifts emerged within a specific political context. The latter has been characterized by decisions adopted by the Turkish government that, as already highlighted in the

contextualization, have eroded the country's judicial independence, have maintained the government's grip on regulatory bodies like the RTÜK (Radio and Television Supreme Council) and BDK, and have also blurred the limits of illegal context in the country (through different clauses of the Turkish Penal Code the Anti-Terrorism Law) (Balamir Coskun, 2021). As a direct result of the explained amendments and the political and legal context which has seen Turkey becoming one of the countries jailing the most journalists in the world (Balamir Coskun, 2021), it is evident that Ankara has increased its power, control and pressure on social media outlets as well as users. Thus, these dynamics point out not only to Turkish cyberspace's further territorialization, but also to its politicization. In addition and bearing in mind that these kinds of legal changes were unsurprisingly justified with security reasons, it becomes clear that the approach reflected by Turkey's amendments align with the one embraced by SCO's states such as China and Russia. Countries which have been favoring a highly controlled Internet which has been also directed to further territorialize their respective cyberspace and silencing online political insurrections (Liaropoulos, 2016). It is this Hobbesian perspective that Eldem had already identified within Turkey's cyber policies, which was indeed strengthened through the "Social Media" and "Civil Society" Laws. Therefore, I argue that these dynamics highlight again Ankara's further turn towards a multilateral and specifically a state-centered approach (and its distancing from multi-stakeholderism), by which freedom of expression and independence within social media have been weakened. This also shows the correlation between Turkey's rising authoritarianism and the Turkish state's quest and successful intent for increasing its control in cyberspace.

The "Disinformation Law" as Ankara's other major step towards multilateralism, digital authoritarianism and the state-centered approach

In this part, I will be analyzing the "Disinformation Law", which was passed by Erdogan in October 2022. Since the regulation of cyberspace and specifically social media is a fundamental aspect in a country's cyber governance, this mentioned law and its consequences need to be studied. The amendments encompassing the mentioned law, which were justified by referring to the danger

of disinformation and the relevance of the country's security and stability, led to a great increase of the Turkish state's control of the Internet and social media platforms. Apart from showing Ankara's alignment with the multilateral and state-centered model, it also depicts its rising cyber-authoritarianism, which makes even more sense considering the already explained Turkey's authoritarian political turn by the hand of Erdogan's AKP. Therefore, this chapter does also reflect the correlation between cyber governance multilateral and interventionist measures and authoritarianism.

The so-called "Disinformation Law" which was pushed by Turkey's ruling Justice and Development Party (AKP) and its junior partner, the National Movement Party (MHP), was signed into law by Erdoğan on October 18 2022 (Coşkun, 2022). This law, which President Erdogan had himself proposed, builds on the already explained 2020 amendment and amended 40 existing laws, such as the Electronic Communication Law, the Internet Law, the Press Law, and the Turkish Penal Code (Global Encryption, 2023, Knodel, 2022, Human Rights Watch, 2022). It is important to highlight that the rising concerns over the laws' authoritarian nature nor the request to the Constitutional Court by the main opposition party of the Republican People's Party (CHP) were able to avoid the bill from being passed (Coşkun, 2022) (Esen, 2022).

First of all, the mentioned amendments, which build on the 2020 laws, led to the formalization of tech companies' status in Turkey. Despite the 2020 requirement towards the companies with over 10 million daily users to form representative offices or elect real person representatives, the 2022 Disinformation Law increased the extent to which these companies can be criminally, administratively and financially liable. By doing so and since 2022, tech companies are expected to set up companies within Turkey. By doing so, Ankara would be closing a loophole in the 2020 amendments that was exploited by big tech companies such as Facebook and Twitter. Despite appointing or establishing legal companies, the latter were not having genuine legal connection to them. The new requirement needs to be satisfied by firms within six months. If it is not satisfied, companies are punished with advertisement bans and bandwidth up to 90 percent (Human Rights Watch, 2022).

Under this “Disinformation Law”, OTT services, which include a broad range of Internet-based services encompassing email providers, social media companies and providers of messaging services (Global Encryption Coalition, 2023), are forced not only to identify users accused of certain crimes but also to share user data with courts and prosecutors if requested. In addition and in relation to the law’s referral to “content endangering the security of life or property”, social media companies are also expected to report any content falling into this category and to inform the responsible institutions about the users behind it. Due to the mentioned category’s undefined nature, it has not been fully clear which kind of content social media platforms will need to monitor and disclose (Human Rights Watch, 2023). Added to that, OTTs are also required to disclose traffic data. However, since user’s communications are usually end-to-end encrypted, it is not clear how OTTs will be able to access their users’ content without undermining their respective security and privacy (Global Encryption Coalition, 2023).
In case of non compliance with blocking or removal decisions (Human Rights Watch, 2022), the mentioned platforms are subject to heavy fines (Coşkun, 2022) and can be also punished with the reduction of their bandwidth (explicar en nota a pie de página que es). While there can be up to six-month bans on receiving advertising and 50 percent bandwidth reduction, the latter could be raised to 90 percent after 30 days of non-compliance. Social media platforms could be also fully blocked. Concerning the fines, which can only be issued by BTK’s President, they can be up to 3 percent of the global turnover in the previous year (Human Rights Watch, 2022).

Furthermore, the bill also includes a prison sentence of up to three years for publishing misleading information related to the internal and external security of the country, public order and health (Esen, 2021). Apart from this, the law also punishes the “intent to cause fear or panic”. All these offenses are the ones which serve as the basis for criminal charges (Coşkun, 2022). The BTK, which is the institution responsible for giving licenses to messaging companies by which they could operate, has also developed secondary regulations which specify the conditions under which communication companies would need to intercept, access or disclose private conversations (Human Rights Watch, 2023). In relation with the mentioned institution, although it operates under the Ministry of

Transport, the BTK lacks independence and its decisions are not subject to a great judicial oversight. Additionally, President Erdogan is the ones selecting its president and members (Human Rights Watch, 2022).

Concerning the last relevant aspect of this law there is its intent to make the Press Law applicable to online news sites. The amendment did not only extend card requirements to journalists working for internet news sites, but it also included the restructuring of the cards' issuing and the possibility of being deprived from this permission in case of violating "media ethics". This can also include journalists' long-term inability to reapply to receive these cards. Under this law and with the aim of being able to send legal notifications such as court summonses electronically, online news sites are also required to include contact information on their main page. Last but not least, the former are also obliged to save their online content for two years (Human Rights Watch, 2022).

In relation to this law's consequences, since social media platforms are forced to identify users and also share their data with courts and prosecutors, Turkish individuals and organizations running online accounts (especially if they are critical with the government) are much more exposed (Human Rights Watch, 2023). This is because the amendments have made it far easier for authorities to monitor and remove content from social media platforms and also to prosecute individuals promoting specific views (Esen, 2022). Therefore, the law does not only increase the state's control over social media platforms and online news sites, but it also threatens and limits freedom of expression (Coşkun, 2022, 2022).

Another relevant effect of the amendments is that they will likely create fear among Turkish citizens who could potentially start to censor themselves. This threatening character of the Disinformation Law towards the right to freely express certain critical opinions has been also highlighted by the government's capacity to make use of state accreditation and advertising rights to intimidate individuals and organizations (Esen, 2022). In addition and due to the ambiguous nature of the mentioned offenses that will be use in criminal charges around "the possibility to mislead the public", "public order and health", "internal and external security" and "the intent to cause fear or panic" (Coşkun, 2022, 2022, Esen,

2022), it is evident that there is no single objective interpretation of them so that they could also be potentially used politically and strategically by the Turkish state (as the vague wording could facilitate the criminalisation of any “uncomfortable opinion”). This danger increases if we consider Turkey’s recent authoritarian turn, characterized by an increasingly politicized judicial branch and the lack of independence of relevant institutions, especially in this field, such as the BTK. This particular context and the law’s potential negative impact on public debate was also reflected by the great resistance the bill encountered from opposition parties and other stakeholders which are specifically influenced by it such as journalists and civil society. The latter were also not consulted concerning the legislation (Coşkun, 2022, 2022, Esen, 2022). Due to these different developments, the mentioned bill seems to threaten freedom of expression and privacy (Human Rights Watch, 2023).

On the other hand, concerning the social media platforms' new requirement of disclosing traffic data and accessing users' content, there is a great risk that by doing so, users’ security and privacy will be undermined. This is because their communications are usually end-to-end encrypted. Due to the fact that the latter is a high-level security technology which makes intended recipients the only able to decrypt the message, OTTs using end-to-end encryption could become inaccessible in Turkey (as they would be technically unable to comply with this new law) (Global Encryption Alliance, 2023). A potential secondary legislation forcing providers of end-to-end encrypted services such as WhatsApp, Signal and Telegram Secret Chat to disclose messages (Human Rights Watch, 2023) would push them to choose to either undermine their users’ security or abandon the Turkish market (Global Encryption Alliance, 2023). End-to-end encryption is fundamental to Turkey’s economic and security success because a lack of security and privacy could increase foreign corporate espionage towards Turkish companies. That is why the mentioned provision could indeed negatively affect non-state stakeholders such as the Turkish private sector, specifically the defense industry (due to its role in national security and defense), and civil society (ibid). Last but not least and by threatening anonymity, these amendments do also threaten the ability to express critical opinions (Human Rights Watch, 2023),

which could further lead to an even more authoritarian context with a more critical lack of dissenting voices within Turkey.

Regarding these amendments' more general impact and meaning as well as their relation to the main cyber governance models, it is worth noting that they have undoubtedly led to a major shift within Turkey's media and social media landscape. The fact that social media companies are now required not only to be fully established in Turkey as companies but also to monitor and disclose information about their users and that any content "intended to cause panic of fear" and threatening the country's stability constitutes a crime, it has without any doubt further endangered freedom of expression and public debate within Turkey. Of course it cannot be denied that all states are developing numerous policies and directing their focus towards the phenomenon known as "disinformation", but it is also true that interventionist laws and criminal offenses with certain vague words can be strategically and politically exploited by governments in power. This becomes even more potentially important if we talk about a country whose leader and government have strengthened its grip on the state and has turned more authoritarian.

In addition, bearing in mind that most of Turkey's media outlets are controlled by the ruling Justice and Development Party, it also draws our attention to how much opposition (from opposition parties as well as journalists and civil society) the disinformation law faced. This clearly highlights the relevance of this law and its consequences and how aware were certain actors within Turkey about the potential politicization of this law and how the former could be instrumentalized by the government to repress critical voices. This is even more important in the Turkish context, in which social media had already become the safest space in which alternative views could be freely expressed (specifically in critical political moments such as elections) (Coşkun, 2022).

Concerning the amendment that would require social media platforms to access users' content which would also imply in some cases breaking the end-to-end encryption, it is important to mention that this law would not only weaken users' security and privacy and thus also the space for public debate, but also the Turkish private sector. This is because end-to-end encryption is also relevant for

the confidentiality of companies' information. Thus, considering that this law was justified by the danger that disinformation represents and the great cybersecurity threats that Turkey faces (Global Encryption Alliance, 2023); it seems a bit paradoxical that the same law could indeed have a negative impact on Turkish companies' and specifically the defense industry's security. Aspects which could have negative economic consequences. Based on this and despite the fact that we cannot offer a direct proof for that, it seems that the Disinformation Law was mainly directed towards the control of the domestic media and information landscape rather than strengthening the country's general cybersecurity. This quest by the Turkish government for increasing its control of the country's cyberspace could indeed also include the already mentioned political calculations and the intent to maintain the grip on power. This is a phenomenon which was already explained in the literature review and which is described by Belli (2021). Last but not least, the context and the way in which the mentioned bill was passed as well as its potential negative effects on social media platforms and other companies operating in the country could also reflect the little or lack of influence non-state stakeholders (as the ones mentioned) had concerning this legislation.

As a conclusion and based on how much this law strengthens the Turkish state's control over the Internet, how it diminishes users' anonymity and to an extent freedom within social media, how it weakens a space for expressing alternative views, and how it could also negatively affect companies' security and privacy; I argue that this bill is an evident reflection of the multilateral approach and that it could also have a correlation with AKP's intent to reinforce its power (which should not be difficult considering the politicization of Turkey's judiciary). Since Turkey's "external security and public order" are introduced to identify whether users' content constitute any criminal offense, and social media platforms (which tend to be foreign) are even more controlled by the Turkish state, I also argue that the mentioned law perfectly aligns with the idea of digital sovereignty and the state-centered approach. Indeed, this becomes even clearer not only due to Ankara's prioritization of control over liberties in cyberspace, but also if we see the Disinformation Law, as the culmination of the Turkish state's prolonged effort to control cyberspace. Process which started with the previously discussed 2020

“Social Media and Civil Society Laws” and with this last law seems to reach a successful end (for the ruling party).

Conclusion

After having analyzed Turkey's 2020-2023 NCSS document as well as its different regulations and the country's relationship with other states, organizations and conventions; it becomes necessary to summarize the most relevant findings and give an answer to the research question about the nature of Turkey's cyber governance approach. After that and also based on the analysis and all the findings, I will be also reflecting on broader but relevant topics related to cyber governance that have also come up in this research such as the applicability and realm of the existing cyber governance models and theories, the question around the influence of a given political context on a country's approach, and an apparent international multilateral trend within the governance of cyberspace.

On the one hand and concerning the official document, despite its respective limitations and the unpublished "Action Plan", it is evident that Ankara has embraced a rather broad definition of cyber governance stakeholders. Therefore, apart from identifying state-actors, it also recognizes the role that non-state ones such as private companies, research centers and universities could have in the governance of cyberspace. However, and based on the NCSS document, the only mentioned major and direct contribution of these non-state actors was their feedback function concerning the drafting of the former. Due to this limited responsibility that they seem to have received as well as Ankara's support for the strengthening of international cybersecurity and cyber governance cooperation within a multilateral framework; the NCSS content aligns more with the multilateral cyber governance model.

On the other hand and in relation to the analyzed post-2020 developments and measures, the findings do also point in the same direction.
Concerning Turkey's relatively close relationship with its NATO partners as well as the EU, it is relevant to highlight that this engagement is carried out by Ankara within a multilateral framework. A perfect example for this is the already mentioned and analyzed Budapest Convention. Despite Ankara's signing

bringing Turkey closer to European and Western countries within the area of cybersecurity and cyber crime cooperation and exchange of information, this did not include any requirement nor need for the signing parties to change their domestic cyber governance approach and policies. This is because the cooperation is based on a multilateral engagement. As a result, while this convention has been mainly signed by European and Western states or states with close relation with them, it would be perfectly compatible to be a country with a highly interventionist and multilateral cyber governance approach and be at the same time a Budapest Convention's party. Thus and since a multilateral type of cooperation hardly threatens the idea of sovereignty and Turkey had already relatively close relations with the European community and Washington, I argue that Ankara's decision to be a party of the Budapest Convention reflects a coherent behavior guided by its interest to avoid giving up any degree of sovereignty and protect it at all cost by avoiding multi-stakeholder and supranational interactions Additionally, the mentioned convention does also serve its pragmatic interests of increasing Turkey's cybersecurity and maintaining close and beneficial relations with relevant actors such as NATO allies and Europe. Therefore, I argue that despite Western and European countries' traditional support of multi-stakeholderism, Turkey's close relationship with them and its participation in the convention do not reflect any "multi-stakeholder turn" by Ankara at all.

In relation to Turkish non-state actors' role within the country's governance of cyberspace, I have found that despite Ankara's promotion of public-private cooperation and non-state actors' role and contribution in different cybersecurity areas, these actors have lacked influence and a relevant role in cybersecurity state institutions and cyber governance decisions and measures. Therefore and although the private sector and academia have had an active and autonomous role in areas such as education, the mentioned dynamic highlights Ankara's inclination to reserve any relevant decision-making process and the design and approval of cyber governance measures exclusively to state institutions, reflecting an evident multilateral approach.

Moreover, Ankara's decision to update its PDPL, largely inspired and influenced by the EU's GDPR, reflects Turkey's full embracement of the idea of "digital sovereignty", the need to strengthen it as well as its active behavior to protect the country's sovereignty and autonomy within cyberspace and the data realm. Therefore and taking into account that GDPR's raison d'être has been the strengthening of EU's digital sovereignty and the intention to limit foreign companies' power and influence vis-à-vis EU citizens, the market and state institutions, and that Turkey's measures seems to logically purse the same objectives; PDPL's update represents a highly interventionist, sovereigntist and protectionist measure. Again, these objectives, dynamics and realm behind Turley's PDPL point out again towards the multilateral approach, characterized by its strong prioritization of sovereignty's protection and a certain mistrust of external and foreign actors (also including private companies).

Last but not least and regarding the different implemented amendments since 2020 known as the "Social Media Law", the "Civil Society Law", and the "Disinformation Law", there is no doubt that they led to a major increase in the Turkish state's control of cyberspace and specifically the Internet and social media. While the two first laws strengthened Ankara's power, control and pressure on social media outlets as well as users (with the justification of fighting against cyberbullying, disinformation and terrorist propaganda), the "Disinformation Law" further culminated this process. The latter amendment did not only increase the Turkish states' control over the Internet, but it also diminished users' anonymity and limited freedom of expression within social media. By doing so, the amendment, which could at the same time have the negative impact of weakening companies' security and privacy, evidently weakened the possibility of using social media to express alternative views. Additionally it should be mentioned that these laws were passed in a particular political context, characterized by a strong opposition against them and AKP's intent to maintain its grip on power. These laws' consequences, especially the ones concerning private companies and social media platforms, clearly reflects not only Ankara's prioritization of state control over liberties, but also its desire to almost fully control the whole media landscape, which is a crucial element for any political actor, especially in an authoritarian context. Therefore, I argue that these

last measures, apart from having a clear multilateral realm, due to its even more interventionist and controlling nature, do also align with the more “radical” state-centered approach.

As a conclusion and based on all these findings, I can claim that the analysis has proved the initial hypothesis that Turkey’s cyber governance approach was not lying in a middle between the two main cyber governance models. Ankara’s most recent approach to govern its cyberspace, characterized by an interventionist, sovereigntist, protectionist and authoritarian nature, does indeed align with the multilateral model and includes even some features from the state-centered approach (such as the fierce control of social media and the media landscape). Therefore and considering that having a close relationship with Western and European states and their institutions within the cybersecurity area (such as the case of Turkey) does not serve as any proof for an alignment with multi-stakeholderism, there is sufficient evidence (in opposition to what Eldem claimed in 2020 and 2021) highlighting Ankara’s full departure from the multi-stakeholder cyber governance model. Despite being a secondary finding, the research has also shown the potential correlation between certain amendments (such as the “Disinformation Law”) and Turkey's current authoritarian political context characterized by the current government’s strong prioritization of the country’s “security, independence and stability”, a weakened system of check and balances and judicial independence, and its intent to maintain its grip on power by all costs.

Apart from the proved hypotheses, the study’s findings have also shed light on other relevant topics related to cyber governance which need to be mentioned.
First of all, the study has shown the great similarity there is between the approaches adopted by the EU and Turkey respectively. By embracing the idea of digital sovereignty and also the need to protect it, both actors have developed interventionist policies seeking to safeguard their respective autonomy and sovereignty in fields such as the data realm as well as to limit external actors’ influence within their respective borders. Therefore and taking into account that the EU has been often considered a liberal and democratic example, it becomes strictly important and interesting to study how actors with such apparently divergent formal political systems, have ended up adopting very similar

cybersecurity and cyber governance policies. This has been even further reinforced by the fact that it is not Turkey which has turned towards a multi-stakeholder approach, but the EU which has been supporting the idea of sovereignty and autonomy and supporting status and interventionist measures and has even served Ankara as a source of inspiration and influence.

This case reinforces two relevant reflections that need to be expressed. On the one hand, the fact that actors with such a divergent political situation end up implementing highly similar cyber policies and adopting a similar cyber governance approach, could highlight the potential lack of relevance of “formal political features” in understanding and analyzing a country’s governance of cyberspace. On the other hand, the fact that the EU, often recognized for its liberal and democratic realm and that has often supported the multi-stakeholder approach (and thus the idea of overcoming borders and including non-state actors in cyber governance) has been adopting a multilateral cyber governance, is also indeed an interesting development (perhaps for some contradictory) which makes me formulate the following question: If there is a major trend towards a multilateral approach and interventionist and sovereigntist policies also by the states that where theoretically more aligned with multi-stakeholderism, is the latter model really being applied? This makes us think to what extent is the multi-stakeholder cyber governance model “real” and is really being adopted by any state.

Last but not least, following the critics of many states towards multi-stakeholderism as a US-centric approach and also the characterization made by several scholars of it as “US discursive tool” employed by Washinton to build an hegemonic discourse to sustain a system favoring its interests (Bourdieu, 1977, Carr, 2015, Chenou, 2014, Gramsci, 2001); it becomes fundamentally necessary to further study this topic and contrast whether the latter could be the case. This is indeed of fundamental importance, as the multi-stakeholder model, as one of the main theoretical frameworks in the field of cyber governance, is a relevant tool to study these topics. It is evident that in case the idea developed by Bourdieu, Carr, Chenou, and Gramsci would be further proven, there would be

an urgent need to study and develop other theories more applicable to study the cyber governance field.

Bibliography

- Akçay, Ü. (2021). Authoritarian consolidation dynamics in Turkey. *Contemporary Politics*, *27*(1), 79-104.
- Akkoyunlu, K., & Öktem, K. (2018). Existential insecurity and the making of a weak authoritarian regime in Turkey. In *Exit from Democracy* (pp. 37-60). Routledge.
- Akyeşilmen, N. (2022). Türkiye in the Global Cybersecurity Arena. *Insight Turkey*, *24*(3), 109-134**.**
- Ali, H. M. (2021). 'Norm Subsidiarity' or 'Norm Diffusion'? The Journal of Intelligence, Conflict, and Warfare 4 (1): 122–48.
- Aslan, B. (2020). Who will Govern the Cyberspace? A Debate on Multi-stakeholderism vs. Multilateralism. *Horizon Insights*, 31.
- Association for Progressive Communications (APC) and Swedish International Development Cooperation Agency (Sida). (2022). Global Information Society Watch 2021-2022 Digital futures for a post-pandemic world. Extracted from https://gisw.org/sites/default/files/GISWatch2021-22.pdf
- Balamir Coskun, G. (2021). Turkey's New Internet Law and Its Effects on Freedom of Media. *Reset Dialogues on Civilizations.* Extracted from https://www.resetdoc.org/story/turkey-internet-law-freedom-media/
- Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security*, *31*(3), 356-376.
- Belli, L. (2021). BRICS countries to build digital sovereignty. *CyberBRICS: Cybersecurity regulations in the BRICS countries*, 271-280.
- Bourdieu, P. (1977). *Outline of a theory of practice*. Cambridge: Cambridge University Press.
- Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261-1280. Extracted from https://scholar.google.com.mx/scholar?cluster=5934901776676529535&hl=es&as_sdt=0,5
- Carr. (2015). Power plays in global Internet governance, Millennium: Journal of International Studies, vol. 43, no. 2, pp. 640-59. Extracted from https://scholar.google.com.mx/scholar?cluster=16390736015310853705&hl=es&as_sdt=0,5
- CCDCOE (NATO Cooperative Cyber Defense Centre of Excellence). (2023). World's largest cyber defense exercise Locked Shields kicks in Tallinn. Extracted from https://ccdcoe.org/news/2023/worlds-largest-cyber-defense-exercise-locked-shields-kicks-off-in-tallinn/
- Chambers and Partners. (2023). Cybersecurity 2023: Definitie Global law guides offering comparative analysis from top-ranked lawyers. Extracted from https://chambers.com/downloads/gpg/771/015_turkey.pdf
- Chang, L. Y., & Grabosky, P. (2017). The governance of cyberspace. *Regulatory theory: foundations and applications*, 533-551. Extracted from https://www.researchgate.net/profile/Lennon-Chang/publication/314231806_The_governance_of_cyberspace/links/58e42dc5aca272d629779ee5/The-governance-of-cyberspace.pdf
- Chen, X., & Yang, Y. (2022a). Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. *The International Spectator*, *57*(3), 1-14. Extracted from https://www.tandfonline.com/doi/full/10.1080/03932729.2022.2101231
- Chen, X., & Yang, Y. (2022b). Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *THE INTERNATIONAL SPECTATOR*, *57*(3), 48-65. https://www.iai.it/sites/default/files/tis_2022_3_chen_yang.pdf
- Chenou, J. M. (2014). From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalization of internet governance in the 1990s. *Globalizations*, *11*(2), 205-223.

- Çifci, H. (2024). Analysis of Türkiye's Cybersecurity Strategies: Historical Developments, Scope, Content and Objectives. *Sakarya University Journal of Science*, *28*(1), 203-219. Extracted from https://dergipark.org.tr/en/download/article-file/2946908
- Coşkun, A. (2022). Turkey's New Disinformation Law Affects More Than Meets the Eye. *Carnegie Endowment for International Peace*. Extracted from https://carnegieendowment.org/2022/12/19/turkey-s-new-disinformation-law-affects-more-than-meets-eye-pub-88633
- Council of Europe. (n.d.). The Budapest Convention (ETS. No. 185) and its Protocols. Extracted from https://www.coe.int/en/web/cybercrime/the-budapest-convention
- Council of Europe. (n.d.). Turkey. Extracted from https://www.coe.int/en/web/octopus/-/turkey
- Cybercrime Convention Committee. (2020). The Budapest Convention on Cybercrime: benefits and impact in practice. *Council of Europe.* Extracted from https://es.search.yahoo.com/search?fr=mcafee&type=E210ES885G0&p=Budapest+Convention+and+mult-stakeholderism
- De Gregorio, G., & Radu, RRadu. (2022). Digital constitutionalism in the new era of Internet governance. International Journal of Law and Information Technology, 30(1), 68-87.
- Deibert, R. J., & Pauly, L. W. (2019). Mutual entanglement and complex sovereignty in cyberspace. In *Data Politics* (pp. 81-99). Routledge.
- DW. (2020). "User safety or censorship? Turkey targets social media platforms". *DW.* Extracted from https://www.dw.com/en/user-safety-or-censorship-turkey-targets-social-media-platforms/a-55150477
- Ebert, H., & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, *34*(6), 1054-1074.
- Eldem, T. (2021). Between Multi-stakeholderism and Cyber Sovereignty: Understanding Turkey's cybersecurity strategy. In Routledge Companion to Global Cyber-Security Strategy (pp. 395-408). Routledge.
- Eldem, T. (2020). The governance of Turkey's Cyberspace: between cyber security and information security. International Journal of Public Administration, 43(5), 452-465.
- Erdem & Erdem. (2020). Regulations on Social Media and Internet Contents Through Law No. 7253. Extracted from https://www.erdem-erdem.av.tr/en/insights/regulations-on-social-media-and-internet-contents-through-law-no-7253
- Erdoğan, B. (2021). Data Protection Around the World: Turkey. In *Data Protection Around the World: Privacy Laws in Action*. TMC Asser Press. https://link.springer.com/chapter/10.1007/978-94-6265-407-5_9
- Erensü, S., & Alemdaroğlu, A. (2018). Dialectics of reform and repression: Unpacking Turkey's authoritarian "turn". *Review of Middle East Studies*, *52*(1), 16-28.
- Ergöçün, G. (2021). Turkey: Malware attacks up to 81% in 2020. Anadolu Agency. Extracted from https://www.aa.com.tr/en/science-technology/turkey-malware-attacks-up-81-in-2020/2105600
- Esen, B. (2022). Turkey's New Disinformation Law: An Alarming Trend Towards Cyber-Authoritarianism. *Stiftung Wissenschaft und Politik.* Extracted from https://www.swp-berlin.org/publikation/turkeys-new-disinformation-law-an-alarming-trend-towards-cyber-authoritarianism
- European Commission. (2022). Türkiye 2022 Report. Extracted from https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/T%C3%BCrkiye%20Report%202022.pdf
- European Parliamentary Research Service. (2020). Digital Sovereignty for Europe. Extracted from https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
- Franceschini, J. and Falduti, M. (2023). *Conceptualizing Cybercrime across Four Mediterranean Countries. Preliminary Analysis of Regulation and Policies in Israel, Italy, Spain and Turkey.* In Arrigo, G., M. and Franceschini, J. (Eds.), *Revolutionary Times, Mediterranean Perspectives* (1st Edition, 113-134). Aracne Publishing, Rome.
- GDPR.EU (n.d.). What is GDPR, the EU's new data protection law? Extracted from https://gdpr.eu/what-is-gdpr/

- Global Encryption Coalition. (2023). Over 40 organizations and cybersecurity experts call on the Turkish government not to undermine end-to-end encryption. Extracted from https://www.globalencryption.org/2023/04/over-40-organizations-and-cybersecurity-experts-call-on-the-turkish-government-not-to-undermine-end-to-end-encryption/
- Gramsci, A. (2001). *Selections from the prison notebooks of Antonio Gramsci*. London: Electric Book.
- Güven Tastan, F. (2024). Turkey's data protection amendments for 2024: A closer look. The International Association of Privacy Professionals. Extracted from https://iapp.org/news/a/turkeys-data-protection-amendments-for-2024-a-closer-look/
- Halisdemir, E. (2021). National Cybersecurity Organisation: Turkey. NATO CCDCOE, National Cybersecurity Governance Series, Tallinn. Extracted from https://ccdcoe.org/uploads/2021/08/TUR_country_report_final_clean_ver_2408.pd
- Human Rights Watch. (2022). Turkey: Dangerous, Dystopian New Legal Amendments. Extracted from https://www.hrw.org/news/2022/10/14/turkey-dangerous-dystopian-new-legal-amendments
- Human Rights Watch. (2023). Questions and Answers: Turkey's Control of the Internet and the Upcoming Election. Extracted from https://www.hrw.org/news/2023/05/10/questions-and-answers-turkeys-control-internet-and-upcoming-election#_Toc134065371
- IISS. (2023). Cyber Capabilities and National Power Volume 2. Extracted from https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/
- ISPI. (n.d.). In Cybersecurity, Turkey Leads the Way. Retrieved from https://www.ispionline.it/en/publication/cybersecurity-turkey-leads-way-35348
- ITU. (2017). Global Cybersecurity Index (2017). Extracted from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx
- ITU. (2018). Global Cybersecurity Index (2018). Extracted from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx
- ITU. (2020). Global Cybersecurity Index 2020 Report. Extracted from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx
- Kadlecová, L. (2024). *Cyber Sovereignty: The Future of Governance in Cyberspace*. Stanford University Press.
- Karataş, A. (2020). The comparative analysis of national cyber security policies: United States, United Kingdom and Turkey examples. *Journal of Academic Social Resources*, *5*(19).
- Kim, S. (2022). Roles and Limitations of Middle Powers in Shaping Global Cyber Governance. The International Spectator 57 (3): 31-47.
- Knodel, M. (2022). Turkey's authoritarian slide takes aim at encryption. *Global Encryption Coalition.* Extracted from https://www.globalencryption.org/2022/10/turkeys-authoritarian-slide-takes-aim-at-encryption/
- Liaropoulos, A. (2016). Exploring the complexity of cyberspace governance: state sovereignty, multi-stakeholderism, and power politics. *Journal of Information Warfare*, *15*(4), 14-26. Extracted from https://www.jstor.org/stable/pdf/26487548.pdf?refreqid=fastly-default%3A231edf8d667b29c8cac38b215dfe11a4&ab_segments=&origin=&initiator=&acceptTC=1
- Liaropoulos, A. (2017). Cyberspace governance and state sovereignty. *Democracy and an open-economy world order*, 25-35. Extracted from https://link.springer.com/chapter/10.1007/978-3-319-52168-8_2
- Liaropoulos, A. (2021). EU Digital Sovereignty: A Regulatory Power Searching for Its Strategic Autonomy in the Digital Domain. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security*. Academic Conferences Inter Ltd..
- Machado, M. N. C. (2015). Cyber security governance. Extracted from https://scholar.google.com.mx/scholar?hl=es&as_sdt=0%2C5&q=Machado%2C+M.+N.+C.+%282015%29.+Cyber+security+governance.&btnG=

- Maurer, T. & Morgus, R. (2014). Tipping the scale: An analysis of global swing states in the internet governance debate. Extracted from https://www.cigionline.org/sites/default/files/no7_2.pdf
- (MTI) Republic of Turkey, Ministry of Transport and Infrastructure. (2020). National Cybersecurity Strategy 2020-2023. Extracted from https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf
- Örmeci, O., Yılmaz, E. A., & Köker, A. E. (2022). Turkey's cyber security policies.
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Pohle, J. & Thiel*. Extracted from https://pdfs.semanticscholar.org/9f4e/3203f2d4b39cace023a11f24d03fa0bf618a.pdf
- Presidency of the Republic of Turkey, Digital Transformation Office. (n.d.). Projects. Extracted from https://cbddo.gov.tr/en/projects/#6233
- Rebello, K. (2017). Building Walls with 'BRICS'? Rethinking Internet Governance and Normative Change in a Multipolar World. Working Paper 1 (1). St. Andrews: Centre for Global Constitutionalism.
- Reuters. (2020). "Turkey determined to control social media platforms, Erdogan says". *Reuters.*
- Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, *1*, 81-93.
- SOCRadar. (2021). 2021 Top Cyber Threat for Turkey. Extracted from https://socradar.io/wp-content/uploads/2022/02/2021-Turkey-Threat-Landscape-Report-ENG.pdf
- Tabansky, L. (2021). Cybersecurity in Israel: Strategy, Organization, and Future Challenges.
- Tansel, C. B. (2018). Authoritarian neoliberalism and democratic backsliding in Turkey: Beyond the narratives of progress. *South European Society and Politics*, *23*(2), 197-217.
- Tencent Research Institute (2021). From Internet Governance to AI Governance. *Artificial Intelligence: A National Strategic Initiative*, 275-279.
- Timucin, F. (2021). 8-Bit Iron Fist: Digital Authoritarianism in Competitive Authoritarian Regimes: The Cases of Turkey and Hungary. Extracted from https://research.sabanciuniv.edu/42417/
- Towers, J. (2014). Internet Governance – Order Out Of Chaos by Judy Towers A Capstone Project Submitted to the Faculty of Utica College August 2014 In Partial Fulfillment of the Requirements for the Degree of Master of Science in Cybersecurity.
- TurDef Global Defence News. (2022). The Turkish Team placed ninth in NATO Cyber Security Exercise. Extracted from https://turdef.com/article/the-turkish-team-placed-ninth-in-nato-cyber-security-exercise
- Weiss, M., & Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. *Governance*, *32*(2), 259-275. Extracted from https://onlinelibrary.wiley.com/doi/epdf/10.1111/gove.12368?saml_referrer
- Yılmaz, Z. & Turner, B. S. (2019). Turkey's deepening authoritarianism and the fall of electoral democracy. *British Journal of Middle Eastern Studies*, *46*(5), 691-698.
- Zhang, Q. (2019). China's Internet Governance: A New Conceptualization of the Cyber-Sovereignty Model.