University of Twente

Drienerlolaan 5, 7522 NB Enschede

Management, Society, and Technology

Component: Bachelor Thesis

From Rising Power to Cyber Influencer?

China's Norm Entrepreneurship in Global Cyber Governance through Cyber Sovereignty and Multilateralism

Unraveling China’s Impact on Kenya's Domestic Regulatory Framework

Berit Schaffer

Date: 28th June 2023

1st Supervisor: Dr. Azadeh Akbari

2nd Supervisor: Dr. A.J.J. Meershoek

Word count: 10.600

Abstract

The fragmentation of global cyber governance is prevailed by powerful states that attempt to persuade norm regulation favoring their national interest. This paper scrutinizes China's role in global cyberspace as a rising economic power attempting to contest Western hegemonic structures and promulgate its model of cyber governance. Hereby, the theoretical framework of the Norm life cycle is utilized to analyze China's norm entrepreneurship. Specifically, the paper refers to the concepts of Chinese cyber sovereignty and multilateralism. Kenya is selected as a case that heavily cooperates with China in infrastructure projects to explore its regulatory framework. Qualitative content analysis is applied to analyze Kenyan policy documents to investigate the extent of China's influence on domestic cyber regulations and Kenya's behavior in global cyber governance. The analysis provides the main findings of Kenya's strive to emancipate and strengthen its independence from external influence through enacting domestic data and cyber security regulations that are adapted to the Chinese model of cyber sovereignty to a certain extent. Globally, China and Kenya pursue divergent motives steered by distinctive incentives that disprove the alignment with Chinese multilateralism. The findings allude that Kenya's driving force of participation in global cyber governance is the enhancement of economic growth.

Table of Contents

List of abbreviations and figures

Abbreviations

BRI	*Belt and Road Initiative*
CG	*Cyber governance*
CS	*Cyber sovereignty*
DSR	*Digital Silk Road*
EU	*European Union*
GCG	*Global cyber governance*
ICTs	*Information and Communication Technologies*
IGF	*Internet Governance Forum*
NP(s)	*Norm entrepreneurs*
NLC	*Norm life cycle*
QCA	*Qualitative content analysis*
UN	*United Nations*
US	*United States*
ITU	*Telecommunication and Information Union*
ICANN	*The Internet Corporation for Assigned Names and Numbers*

Figures

1. Introduction

The globalized world we live in is shaped by rapid digitalization, technological development, and advancement of Information and Communication Technologies (ICTs), which are not solely bound to the domestic landscape of a country but rather a global interwoven procedure (Chen & Yang, 2022a). It leads to the establishment of cyberspace, which has become an increasingly pivotal domain in political, economic, and social dimensions that (re)shapes the order of international relations. Hereby, cyberspace becomes increasingly blurred, borderless, and prone to cyber-attacks and data leaks (Zeng et al., 2017; Chen & Yang, 2022b). Thus, as in almost every other policy field, the urgency and matter of international collective regulation and cooperation are inevitable to address cyber threats. Nonetheless, the state of the art of global cyber governance (GCG) seems different. GCG is defined as a concept that regulates cyberspace through the collective decision-making of sovereign nation-states and organizational platforms on the global level (Kim, 2022). Cheng & Yang (2022a) highlight the prevailing fragmentation of GCG due to several actors and norm entrepreneurs (NPs) pursuing divergent interests and stances thereof. Crucially, there is a lack of global cooperation and a clear governance framework that leads to global cyberspace being "seriously unbalanced" (Chen & Yang, 2022b, p. 466; Zheng & Di, 2022).

1.1. Scientific relevance

The rooted problem of GCG fragmentation is dominated by the conflicting interest of powerful actors, mostly sovereign states, whose behavior is steered by their national concerns (Gao, 2022). In dealing with the contestation of GCG, the scientific debate is mostly determined by exploring the behavior of states within the West vs. Non-West paradigm, namely the United States (US) versus China and their allies (Chen & Yang, 2022b). This research paper attempts to contribute to the scientific debate by studying China's GCG model elaborately and analyzing its behavior in the global arena. Since the country developed into a nation-state possessing one of the largest digital ecosystems and powerful tech companies, which is followed by immense growth of digital businesses, exploring China's approach and deeds in the global arena seem academically and politically relevant. Frankly, China aims to contest the Western-centric model of cyber governance (CG) in promoting cyber sovereignty (CS) and multilateralism striving to influence the norm order and structure of GCG (Gao, 2022; Zeng et al., 2017). Therefore, it seems intriguing to study its norm entrepreneurship in GCG. In dismantling China's influence in promoting its model of CG regulation abroad Kenya is selected as a case to analyze its domestic regulatory framework.

The selection of China and Kenya was inspired by the debate which stretches over more than two decades now, dealing with China's economic partnerships and infrastructure projects in Africa, for instance, the Chinese Belt and Road Initiative (BRI) which is elaborated on in the case description of Kenya. It is seemingly fuelled by Western countries' biased stances and fears that China attempts to impose its political system in developing countries to strengthen its global leadership in the digital infrastructure and technology sector (Gagliardone, 2019). Therefore, it is intended to unmask whether China as an NP successfully (re)shapes the domestic regulation of Kenya which appears as a fruitful example of a country that participates in the BRI (Gao, 2022). Thus, conducting research on the given topic of GCG to contribute to the discourse of understanding the behavior of powerful states such as China and their influential persuasive power in global norm regulation becomes essential.

1.2. Research questions and structure of the paper

As the thesis aims to investigate whether China (re)shapes cyber norm regulation in Kenya, the following research question is conducted:

"*To what extent does China as a norm entrepreneur in global cyber governance impact the domestic cyber governance regulation of Kenya?"*

The research question has the character of an explanatory research question to explore and provide a deep understanding of whether China is successful in promoting its CG model abroad, specifically in the case of Kenya. Hence, it is intriguing to analyze the national framework of CG in Kenya and investigate the influential power of Chinese norm entrepreneurship. Two sub-questions were designed, to break down the main research question and guide the research throughout the paper to address the specific aspects of the research interest. The sub-questions are stated as follows:

(1) What is the current state of the art of domestic cyber regulations in Kenya, and how have those been influenced by China in the context of cyber sovereignty and multilateralism?

(2) What incentives is Kenya following in contributing to global cyber governance regulation and for what reason?

As emphasized in the *(1)* sub-question the regulatory framework of Kenya is utilized to identify the national norm regulations Kenya takes up to address domestic cyber insecurity in order to link it to the concepts of CS and multilateralism. Then, the country's logic and incentive for *(2)* norm compliance and cooperation on the global level is explored. Therefore, Kenyan policy documents are employed as the

research data to deliver a sufficient answer to the conducted research questions. Hence, the thesis is structured as follows. Respectively, the main concepts that are indicated in the research question and sub-questions are defined to provide a better understanding of the topic and the scientific problem that is being dealt with. The paper is steered by the theoretical lens of the Norm life cycle (NLC) first introduced by Finnemore & Sikkink (1998). The theory guides the research in investigating the norm development in GCG, scrutinizing China's role as an NP and the possibility of (re)shaping domestic regulations in Kenya. Furthermore, a literature review is conducted on the state of the art of China's approach to CS and multilateralism on the domestic level and the promotion globally. Furthermore, the case of Kenya is touched upon through a short literature review. Qualitative content analysis (QCA) is applied to analyze Kenyan policy documents as textual data in respect thereof. Hereby, the method chosen is structured and elaborated on in describing the case of analysis, the method of data collection, and the analysis guided by the NLC. In the analysis section, the main findings are described and identified followed by discussing and contextualizing the major findings in a broader context and linking the results to the theory of the NLC. Finally, the conclusion provides an answer to the conducted research queries and emphasizes the gap for novel research.

2. Theory

Theory heavily steers the explanatory power and leitmotif of qualitative research that is based on a deductive research approach. As highlighted by Collins & Stockton (2019) "theory is a big idea that organizes many other ideas with a high degree of explanatory power" and "provides a clearly articulated signpost or lens for how the study will process new knowledge" (p.2). Hence, it is fundamental to choose a theoretical framework that guides the research throughout the paper to gain valuable insights and contributes to the chosen theory through qualitative empirical findings.

2.1. Concepts

In giving a comprehensive understanding of the key concepts indicated in the research question and its sub-questions, they must be identified and defined. The main concepts are indicated as follows: *(1) Cyberspace, (2) Cybersecurity, (3) Cyber governance, (4) Global cyber governance, (5) Norm entrepreneurs, (6) Multilateralism, and (7) Cyber sovereignty.*

The development of ICTs, namely tools such as smartphones, digital networks, and computers, is forming (1) *Cyberspace.* Generally, cyberspace is the non-physical sphere in which subjects communicate, exchange information and knowledge, and obtain businesses and services. Globalization, which results in the interconnectedness of digital systems, networks, and devices leads to the interdependence of technological advancement and digitalization of nation-states and forms a *global cyberspace*. Crucially, it shapes the global structure of the internet in which digital communication is performed (Kuehl, 2009; Pratt, 2019). Chen & Yang (2022a) emphasize that cyberspace is prone to "insecurity, crime, and geopolitical competition, as evident in the intensive media coverage of hackers, data loss, leaks of personal information, compromised networks and cyber-espionage" (p. 1). Hence, it is pivotal to regulate cyberspace and address insecurity through the two intertwined concepts of (2) *Cyber security* and (3) *Cyber governance.*

The concept of (2) *Cyber security* indicates the practice of protecting sensitive information, networks, and electronic devices from theft, damage, or unauthorized access. Hence, cyber security develops mechanisms such as cyber capabilities and cyber security strategies to improve technological infrastructure to prevent cyber insecurity (Hurel, 2022). As aforementioned, cyber insecurities and threats transcend from the national to the international level. Therefore, cyber security is not solely an increasing risk to domestic institutions or individuals but rather transformed into a matter of the global community (Savas & Karatas, 2022). Taking (3) *Cyber governance* into consideration authors such as Chen & Yang (2022a) define the term as a policy field that regulates cyberspace through procedures, practices, and policies that protect and regulate digital infrastructure and the use of technology. It addresses cyber threats that affect governments, institutions, and civil society and is shaped by various stakeholders such as state and non-state actors (Savas & Karatas, 2022). CG must be regulated on multiple levels and is determined by the urgency of pursuing global cooperation to establish a common ground of collective decision-making. Thus, cooperating in (4) *Global cyber governance* becomes crucial and unavoidable in dealing with global problems (Chen & Yang, 2022a).

As aforementioned, CG is shaped by several stakeholders and actors on the global level. Thus, the regulation of cyberspace is influenced and steered by (5) *Norm entrepreneurs* such as China, the US, and the European Union (EU). The term is determined by "agents having strong notions about appropriate or desirable behavior in their community" (Finnemore & Sikkink, 1998, p. 896). Hereby, NPs can be academics, diplomats, and politicians but also anyone who possesses the resources to pursue influence (Maurer, 2011). As an NP, China promotes (6) *Multilateralism* as a model of regulating cyberspace through

international agreements and enforcement of norms as international standards. Multilateralism is determined by the concept of state sovereignty in regulating GCG through international platforms (Gao, 2022; Kim, 2022). Furthermore, the term (7) *Cyber sovereignty* demands equal cooperation and state sovereignty in the matter of GCG. As a centralized concept, it empowers sovereign states to regulate cyberspaces free from external influence and "shapes its domestic policy as well as its international cyber diplomacy, in sharp contrast with the free flow of information that is so vital to the US, the EU, and those whose interests align with them" (Gao, 2022, p. 21).

2.2. Theoretical framework

In taking the research question and sub-questions into account, the NLC by Finnemore & Sikkink (1998) was chosen as the best fitting theoretical framework that suits the nature of the research interest aiming to unmask the extent of China's influence in GCG and specifically in the case of Kenya. The NLC is a consolidated theoretical framework for explaining the cycle of norm evolvement in international relations shaped by international organizations and the behavior of powerful nation-states. Specifically, the NLC serves appropriately as a theoretical framework to analyze China's norm entrepreneurship as a nation-state. Furthermore, scrutinizing the stages of norm development is guided by the intention to unmask Kenya's role and concerns in GCG.

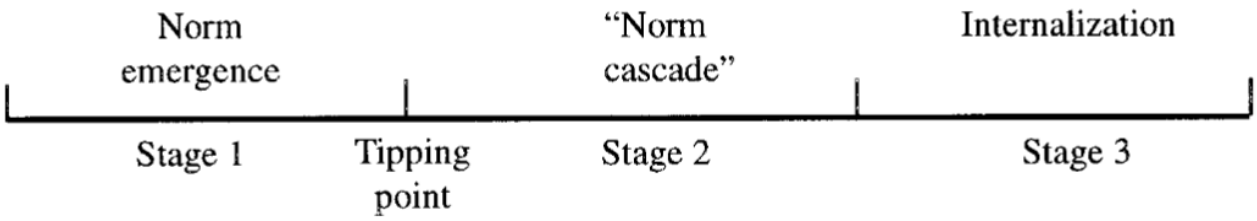
2.2.1. Norm life cycle

The NLC introduced by Finnemore & Sikkink (1998) emphasizes that norms are standard-setters that shape the good-intentioned behavior of states. The two authors explore the internalization, diffusion, and creation of international norms. The theory is largely applied in the academic sphere and is an evident theory in dealing with the evolvement of norms and standards that are shaped by several actors, countries, and stakeholders. They argue that norms are socially constructed and have the power to transform societies and shape behavior. Their theory is based on a three-stage model which is divided into the following three sequences: (1) *Norm emergence,* (2) *Norm cascade, and* (3) *Norm internalization*. The model is constructed in the following: The first stage is indicated as the (1) *Norm emergenc*e in which new norms are introduced as a response to a certain problem or issue. Norms are proposed through various channels by actors and entrepreneurs such as government officials, NGOs, or intellectuals. Therefore, NPs attempt "to convince a critical mass of states (norm leaders) to embrace new norms" and characterize the stage of (1) *Norm emergence* (Finnemore & Sikkink, 1998, p. 895). These norms emerge through acceptance among small groups, for instance, academics, policymakers, and civil society groups.

At this stage, the norm is mostly unknown and lacks acceptance. The first and second stages are divided by a so-called tipping point which is surpassed when the norm becomes (more) widely accepted (Figure 1). The second stage is indicated as the (2) *Norm cascade* in which a larger quantity of actors, including nation-states and international organizations, adopt and adapt to norms. This process is determined by a variety of mechanisms, for instance, the shift of power among states, the replacement of institutional and legal frameworks, or pressure from civil society groups. The norm enhances its influence through the linkage to similar values, norms, or identities of actors which may result in changing behavior and forming policies. Lastly, the stage of (3) *Norm internalization* consists of the acceptance and integration of norms and imitation of behavior. Thus, the norms and values of actors become socially and culturally approved among societies. Finally, the internalized norm develops in the sense of conformity which is reinforced through education, culture, and practices. It becomes a factor of an actor's identity and guides their decision-making and behavior.

Figure 1

Norm life cycle



Note. By Finnemore & Sikkink (1998)

Finnemore & Sikkink (1998), highlight that "new norms never enter a normative vacuum but instead emerge in a highly contested normative space where they must compete with other norms" which is the case in GCG regulations (p. 897). Therefore, the NLC is determined by the *stages of norms* that facilitate norm development in complying with certain factors to overcome norm contestation and become widely accepted. Hereby, the stages of the NLC are "characterized by different actors, motives, and mechanism of influence" that are influenced by specific factors that dominate the process of norm evolvement, acceptance, and diffusion (Figure 2) (Finnemore & Sikkink, 1998, p. 895).

Figure 2

Stages of norms

	Stage 1 *Norm emergence*	*Stage 2* *Norm cascade*	*Stage 3* *Internalization*
Actors	Norm entrepreneurs with organizational platforms	States, international organizations, networks	Law, professions, bureaucracy
Motives	Altruism, empathy, ideational, commitment	Legitimacy, reputation, esteem	Conformity
Dominant mechanisms	Persuasion	Socialization, institutionalization, demonstration	Habit, institutionalization

Note. By Finnemore & Sikkink (1998)

2.2.2. Empirical findings of previous studies

In referring to the behavior of NPs pursuing to influence the stages of norms authors such as Gao (2022) utilize the NLC to dismantle China's role in GCG. He highlights China's attempt to promote and persuade norm development in GCG which is contested by a clash of interests of powerful state agents such as the US and the EU. He emphasizes the shift in leadership and power dynamics and indicates the obsolescence of the debate on norm entrepreneurship in GCG through a West vs non-West lens. Furthermore, he states the convergence of the Chinese and European models in CG. Cheng & Yang (2022b) correspond to the NLC in outlining the urgency for collective decision-making of NPs due to the "effectiveness and legitimacy of global governance call for universally accepted norms; so too does cyber governance" (p. 52). In addition, Glen (2021) applies the NLC in analyzing "Norm entrepreneurship in Global Cybersecurity" and indicates the fragmented state of the art of norm evolvement in GCG hindered by multiple stakeholders following distinctive values and desires (p. 1). As an example, she highlights the failure of the 2016/17 UN GGE conference to regulate nation state's behavior in cyberspace and emphasizes the unlikelihood of a global treaty being implemented soon. Therefore, she emphasizes that the only current mechanisms to

regulate GCG are bilateral, regional, and multilateral cooperation (Glen, 2021). Hereby, taking China's approach to bilateral and multilateral partnerships into account the government collaborates and unites with countries (mostly non-western countries) such as Iran, Russia, and South Africa that hold common interests to facilitate cooperation, legitimacy, and socialization of (2) *Norm cascade* (Gao, 2022). Additionally, Zeng et al. (2017) and Chen & Yang (2022 a) highlight China's attempts to contest the multistakeholderism dominated by the US, in articulating its CG model by taking the lead in regional governance bodies aiming to amend cyber norms. Multistakeholderism is determined as a decentralized concept that builds on the involvement of multiple stakeholders, such as companies, the private sector, and civil society. In contrast to multilateralism, the concept is constructed in a weakened position of nation-states and steered by the principles of freedom and openness (Gao, 2022).

2.3. China's norm entrepreneurship

In outlining China's policy approach as an NP to regulate cyberspace an overview of China's domestic CG model and government bodies is provided, to dismantle China's role as an NP in the global arena. A literature review is conducted to refer to scientific papers published online on China's model of CG regulation and the concepts of multilateralism and CS in GCG. China's GCG approach is assessed as embedded in the stage of (1) *Norm emergence* taking its norm entrepreneurship, motives, and dominant mechanism into account (Figure 2).

2.3.1. China's domestic cyber governance model

As Zeng et al. (2017) and Creemers (2021) highlight the term 'cyber sovereignty' evolved in Chinese articles in 2012 and has been since prioritized as a crucial factor in political matters. It was first promoted in the "White Paper on the Internet in China" (Gagliardone, 2019). Furthermore, internationally the novel term was introduced by Jinping at the 'World Internet Conference' in Wuzhen in 2014 as an approach to global internet governance and international relations. In linking China's approach to CS to its domestic political landscape Zeng et al. (2017) emphasize that one must take the national regulatory framework into account to understand the Chinese foreign policy method due to its steers the country's behavior on the global level. Crucially, China has implemented various measures to censor and control the use of ICTs by its citizens, for instance, through the 'Great Firewall of China' which controls and constrains access to specific websites. The government launched internet platforms such as WEIBO as an equivalent to Twitter and utilizes it for a broad range of purposes, such as, to rule over internet activities. In blocking several

accounts of political activists, the government takes up measures to muzzle opponents. Furthermore, Creemers (2021) deals with China's CG institutions and indicates China's attempts to address the rather fragmented landscape of domestic regulations of cyberspace to enhance its GCG influence through a Cyber Power Strategy that has been developed since Xi took office in 2011. The Chinese institutions regulating CG are ruled from top down by Xi Jinping and consist of an administrative system that is coordinated by several state bodies, ministries, and public-private cooperation, such as the industrial and technical sectors. For instance, the Central Commission for Cybersecurity and Informatization and the Cyberspace Administration of China play a crucial role in developing and enhancing cyber policy adoption and regulation. An example of domestic Chinese cyberspace regulations is the *Cybersecurity law of the People's Republic of China* which was implemented in 2017 (Creemers, 2021). Furthermore, Yang et al. (2023) analyze the development of China's technology-standardized policy system in the time frame from 1978 to 2021. They describe China as a latecomer country that was able to catch up internationally by gaining economic independence, disentangling from foreign technologies, articulating its indigenous standardization approach, and strengthening its capabilities. Thus, the country evolved into a global leader through a "mix of policy tools by referring to the technological capability, economic development level, and institutional environment within that stage" (p. 13). It indicates China's rise in international relations that strengthens its power as an NP.

2.3.2. China's motives in GCG

Chang (2023) deals with the topic of China's discursive power in international relations aiming "to generate a positive image of China globally as well as to fulfill China's strategic objectives" which can be indicated as China's motive of emphatic behavior in the stage of (1) *Norm emergence* (p. 2). Therefore, the country focuses on strengthening its discursive power to enhance its capacity in GCG. Chinese policy documents that were accessible and translated into English on the website of the Ministry of Foreign Affairs of the People's Republic of China (2021; 2023) highlight "China's Positions on International Rules-making in Cyberspace" which state the aim for equal and peaceful cooperation in cyberspace and the importance of coordination on the international level, especially through UN bodies. Therefore, China defines the concept of state sovereignty as interconnected with CS and links its CG model to the Charter of the UN that follows the principle of non-intervention of sovereign states. Therefore, China promotes that international relations and partnerships should "develop universally accepted norms, rules and principles within the framework of the UN, to jointly address the risks and challenges, and uphold peace, security, and prosperity in cyberspace" and "build a global Internet governance system of multilateralism,

democracy and transparency" (Ministry of Foreign Affairs of the People's Republic of China, 2021). Furthermore, the "Chinese Strategy for International Cooperation in Cyberspace" states the four basic principles China follows in GCG: (1) Peace, (2) Sovereignty, (3) Co-governance, and (4) Principle of inclusiveness (Ministry of Foreign Affairs of the People's Republic of China, 2023). China, therefore, aims to promote the development of international rules, national cyberspace sovereignty, economic development, and eradicating the digital divide based on non-interference in another country's internal affairs (Ministry of Foreign Affairs of the People's Republic of China, 2021; 2023). Hereby, China specifies the concepts of CS and multilateralism which are backed by several authors of scientific articles that as well refer to the Chinese models CG (Appendix 1).

2.3.3. China's dominant mechanisms in GCG

Following the stages of the NLC China as an NP attempts to persuade GCG regulation. Therefore, China heavily cooperates with the United Nations (UN), and regional and international platforms pursuing to influence the (1) *Norm emergence* and (2) cascade in GCG (Gao, 2022). As Finnemore & Sikkink (1998) indicate "norm promoters at the international level need some kind of organizational platform from and through they promote their norms" (p. 899). Therefore, it is inevitable to take organizational platforms into account that China may utilize as channels to (re)shape GCG. Crucially, the UN as an international organization is an influential agent in global governance that imposes international laws. Thus, the UN serves as an organizational platform that enables states to act as NPs to (re)shape GCG. Therefore, it is an open space for articulating objectives albeit the prevailing contested landscape and the clash of agendas (Finnemore & Sikkink, 1998). In applying the NLC Maurer (2011) shows "the various signs that norms to govern cyberspace are slowly emerging and moving towards norm cascade", especially while taking the UN as an international platform into account (p. 3). He emphasizes, the General Assembly under the auspices of the UN, that is the only body in international relations that can impose binding international law, in which countries such as Russia, the US, and China attempt to (re)shape cyber laws and resolutions. For instance, China and Russia (and other members) introduced and submitted the 'International Code of Conduct for Information Security' to regulate cyberspace to the UN. It was refused by most Western states and lacked support to reach the tipping point of (2) *Norm cascade* (Maurer, 2011; Gao, 2022). Furthermore, China holds membership in the UN Security Council as one of the five permanent members which empowers China in controversial decision-making and norm development. Furthermore, in listing crucial international platforms that regulate cyberspace, the International Telecommunication Union (ITU) can be emphasized as the only specialized UN agency that is "working on cyber issues with the status

of treaty organization" (Maurer, 2011, p. 29). Hence, NPs such as China utilize the platform to promote their CG approach (Maurer, 2011). Crucially, in taking two other influential organizational platforms that are based on a multistakeholder approach into account, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) can be stated. Gao (2022) and Chen & Yang (2022a) highlight China's opposed stance to ICANN and IGF as non-profit organizations in which the US holds the main power. China especially aims to contest the hegemonic power structure of ICANN which is located in the US.

3. Methods

At first, to provide a brief understanding of the selected case, a description of Kenya is outlined. Furthermore, the section serves to clarify the research design, the method of data collection, and the method of analysis. In referring to the research questions and the theoretical framework the applied method is guided by the lens of the NLC.

3.1. Case description of Kenya

Kenya was chosen due to two main reasons. First, because of its strong economic ties with China through infrastructure projects. Second, in the African context, Kenya has a relatively strong CG framework. Furthermore, the case of Kenya is selected to investigate whether China, especially due to the close economic relationship, is successful in promoting CS and multilateralism in one of its partner countries (Tugendhat & Voo, 2021). Geographically located in eastern sub-Saharan Africa, Kenya's political system is categorized as hybrid and partly free in contrast to the Chinese authoritarian political landscape (Freedom House, 2023a, 2023b). In the sense of domestic cyber regulations Kenya has recently enacted three CG acts (Appendix 2). Hereby, Kenya implemented its first Data Protection Act in 2019 which is "one the most progressive English-language data privacy laws in Africa" and makes it intriguing to analyze the regulatory framework (Greenleaf & Cottier, 2020, p. 7). Furthermore, the Global Cybersecurity Index by the International Telecommunication Union (2020) measured the commitment of 194 countries to address cyber security in which Kenya was ranked 5th in sub–Saharan Africa and worldwide 51st. This indicates Kenya's mainly well-developed CG framework on the African continent. Moreover, Gagliardone & Sambuli (2015) highlight Kenya's dominance as an ICT hub in East Africa that aims to increase its CG resilience to develop into a crucial actor. Moreover, Kenya can be stated as a digital innovation hub which positions the country potentially as a powerful actor in the ICT sector on the African continent

(Gagliardone, 2019). In attempting to unmask the extent of Chinese influence on Kenya's domestic framework it is crucial to consider their economic cooperation. As aforementioned, Kenya and China heavily cooperate through the Chinese BRI and the Digital Silk Road (DSR) (Omolo et al., 2016). Hereby, the BRI interlinked with the Chinese DSR was first introduced in 2015 and can be highlighted as recent projects in which China and African countries actively cooperate in the matter of ICTs, digital infrastructure, and peer learning on CG regulations (Agbebi, 2022). Hereby, LY (2020) and Agbebi (2022) state that the DSR initiative builds on and is embedded in the development of international standards and rules to enforce its goals steered by cooperation in digital connectivity. Given the Kenyan case description regarding its economic ties with China and its CG framework, it is assumed that Kenya is influenced by and imitates the Chinese models (multilateralism and CS) of CG to a certain degree for its own national sake. In addition, it is expected that Kenya strives for cooperation and partnership in GCG through organizational platforms.

3.2. Research design

The method chosen to answer the conducted research question *"To what extent does China as a norm entrepreneur in global cyber governance impact the domestic regulation in Kenya?" and* the two sub-questions *"What is the current state of domestic cyber regulations Kenya, and how have those been influenced by China in the context of cyber sovereignty and multilateralism? What incentives is Kenya following in contributing to global cyber governance regulation and for what reason?"* textual analysis was chosen, specifically qualitative content analysis (QCA). As Given (2008) highlights "Content analysis is the intellectual process of categorizing qualitative textual data into clusters of similar entities, or conceptual categories, to identify consistent patterns and relationships between variables or themes." and is "widely applied in the social sciences whenever textual data are analyzed" (p. 120). Moreover, QCA involves analyzing written or visual communication, such as policy documents, media coverage, or social media posts (Given, 2008). In the case of this paper collecting and analyzing policy documents as textual data is a fruitful method to identify norm regulation approaches and goals of the Kenyan government in CG and GCG. Furthermore, QCA facilities the analysis section to provide a sufficient answer to the research questions in unmasking the extent of Chinese influence as an NP on the Kenyan domestic CG regulations (Given, 2008).

3.3. Method of data collection

The data analyzed are policy documents of Kenya which were collected through desk research. The data is accessed and taken from government websites, inter alia, the parliament, ministries, communication and ICT authorities, and committees. The policy documents utilized are displayed in the **Appendix** to clarify and display the data that is examined. Furthermore, they are cross-checked with legislative documents provided by international organizations, in this case, the United Nations Institute for Disarmament Research (UNIDIR), to ensure their reliability. Crucially, the main Kenyan government bodies that regulate cyberspace are the Communications Authority, Ministry of Information, Communications, and Technology, and National Cybersecurity Authority which are primarily supervised by the national government. The collected policy documents that are assessed in the data analysis section are Kenyan Masterplans, Annual reports, National Policy Guidelines and Strategies, and Data Protection and Cybersecurity Acts (Appendix 2 & 3). The collected documents consist of 8 pieces and vary in terms of length from 15 to 150 pages. Albeit only three documents are CG-related acts while the rest of them encompass policy guidelines and goals (Appendix 2 & 3). Furthermore, the data was collected within the time frame Kenya entered the BRI in 2017 (McBride et al., 2023). Hence, policy documents from 2014 up to 2023 are analyzed to be able to comprehensively indicate the developments and changes in Kenya's domestic cyber regulations and procedures. The analysis includes any policy document that addresses CG regulation, goals, and strategy plans. The textual data, derived from the policy documents, are collected by highlighting textual phrases to create codes aiming to collect patterns and conceptual occurrences to quantify them into (sub-) categories. Therefore, the software tool ATLAS.ti is utilized.

3.4. Method of data analysis

The QCA is applied by following a deductive research approach based on existing theory to develop a coding scheme and link it back to the theoretical framework. Hereby, the coding of the textual data is steered through the lens of the NLC in analyzing the potential internalization of CG regulation. Structuring the coding along the NLC is suitable for discovering and categorizing patterns that allude to China's influence as an NP on cyber norm development in Kenya. In facilitating the coding procedure, the software ATLAS.ti is applied in which the policy documents are uploaded, collected, and coded. Crucially, it is an efficient software that simplifies the search for patterns and to develop a coding scheme. Subsequently, the coding of the policy documents in ATLAS.ti is reasonable in interpreting the results of the analysis considering the NLC, the key theoretical concepts, and referring to the research question and its sub-

questions. Thus, the qualitative data analysis tool is an applicable software to structure and indicate the frequency of codes and group them into categories and subcategories (Saldana, 2016). It facilitates the identification of the regulatory CG approach followed by the Kenyan government and Kenya's participation in GCG. Therefore, the QCA is conducted in the following. Through a deductive coding procedure, the coding scheme fits the structure of the NLC. It follows the method of coding data based on existing concepts or categories according to already consolidated theory (Elo & Kyngäs, 2008). Hence, the coding scheme is applied based on the three key categories of the stages of norms: (1) *Norm emergence,* (2) *Norm cascade,* and (3) *Norm internalization*. This is practical to identify the extent of China's influence through norm entrepreneurship by scrutinizing the domestic norm development, diffusion, and internalization in Kenya (Saldana, 2016). Furthermore, the categories are divided into three subcategories each and are indicated by an attached definition which contains the keywords of the conducted codes. Every subcategory is briefly defined to give a nuanced understanding of the assigned meaning of the codes. In providing examples direct citations for each subcategory are included. Hence, the coding scheme displays the factors that facilitate the support for (1) *Norm emergence* in Kenya through the sub-categories *entrepreneurship, incentive, and persuasion*. The category of (2) *Norm cascade* is divided into the subcategories of an *international organization, legitimacy, and socialization* in showing the factors through which Kenya adapts to and facilitates GCG regulations. Finally, the category of (3) *Norm internalization* consists of the subcategories of *law, conformity, and institutionalization.* The categorization of (1) *Norm emergence* displays Kenya's behavior in GCG that may be (re)shaped by China's model. The stage of (2) *Norm cascade* depicts the factors that facilitate Kenya's approach to norm acceptance and its domestic endeavors to align with GCG. (3) *Norm internalization* indicates the measures Kenya takes up to facilitate domestic norm diffusion. Furthermore, the coding scheme allows the findings to be put in a broader context to identify the concepts of CS and multilateralism and Kenya's participation in GCG (Appendix 4).

Nevertheless, validity and reliability must be assured, especially to make the research comprehensible and replicable. QCA is a subjective and context-related analysis of textual content which is steered by the researcher's interpretation and possibly contains individual biases (Krippendorff, 2004). QCA is applicable in the sense of aiming to understand the meaning of regulations to identify patterns of CG regulation in the policy documents rather than quantifying the findings. Thus, in addressing reliability a comprehensive coding scheme is developed and adapted to the lens of the NLC in distributing the codes among categories and subcategories. In enhancing the validity of the research design, data is collected from multiple databases, in this case, government websites, the UN, and academic literature interlinked with the

consideration of tracing it back to the research questions and contextualizing the findings into the broader scientific debate on GCG (Elo & Kyngäs, 2008).

4. Analysis

This section aims to present and describe the findings of the QCA to indicate to what extent China (re)shapes domestic norm regulations in Kenya and whether the country aligns with China's approach to CS and multilateralism. Thus, the collected findings are connected to China's norm entrepreneurship in GCG and Kenya's behavior is scrutinized in the global arena. It provides an in-depth understanding of Kenya's model of CG regulation and how the country intends to address cyber insecurity. The acquired findings are derived from the policy documents which are displayed in the coding scheme and indicate Kenya's attempt to domestic CG regulation through the lens of the theoretical framework of the NLC (Appendix 4). Significant findings are emphasized through (direct) citations from the policy documents to enhance the explanatory quality of the analysis. Thus, the analysis is divided into three sub-sequences linked to the three stages of the NLC (1) *Norm emergence*, (2) *Norm cascade,* and (3) *Norm internalization* and its subcategories.

4.1. Norm emergence

The first stage of (1) *Norm emergence* is divided into the subcategories displayed in the coding scheme of the NLC *entrepreneurs, incentives, and persuasion* (Appendix 4). The findings indicate Kenya's attempts to contribute to the debate of GCG through participation in organizational platforms to "promote the development and implementation of international laws, agreements, treaties, policies, norms, standards, conferences and fora on cybersecurity" through norm entrepreneurship to develop to an active player in the global arena (National Cybersecurity Strategy, 2022, p. 14). Crucially, the government is driven by the commitment to cooperate with "international partners to improve Kenya's cybersecurity posture" (National Cybersecurity Strategy, 2022, p. 14). Precisely, the National Cybersecurity Strategy (2014) states Kenya's endeavors to enhance CG regulation framed by the incentive of enhancing economic growth in "securing its national cyberspace a national priority to continue to facilitate the economic growth of the country and its citizens" and "advance its socio-economic growth leading to an enhanced quality of life by all the people of Kenya" (p. 5). Thus, the Strategy Paper informs the concerns of the Kenyan government in participating in international platforms to increase GCG cooperation while simultaneously enabling

economic growth to eradicate poverty and transform into a high-income country (The Kenya National ICT Masterplan Towards – a Digital Kenya, 2014; National Cybersecurity Strategy, 2014). Hence, the Kenyan National ICT Masterplan – Towards a Digital Kenya (2014) states the goal of increasing Kenya's persuasion and reputation in global governance. "Kenya is a participant and a signatory to a number of international conventions and standards relating to ICT" and strives to "enhance the international image of Kenya as a digital economy" as a factor to boost economic growth (p. 17).

4.2. Norm cascade

At the second stage of the NLC, the categorization of (2) *Norm cascade* and its sub-categories *states, legitimacy and socialization* are the driving factors that contribute to and shape norm acceptance. As indicated in the theory section and provided by Finnemore and Sikkink (1998), a norm cascades in surpassing the tipping point due to becoming widely accepted by divergent stakeholders such as nation-states and international organizations. The Annual Report, Fostering Digital Transformation through Building a Connected Society, Enabling Regulation, Partnership, and Innovation (2021) provides insights into Kenya's domestic CG approach that is steered by the interest of cooperating on the regional and global level through "established partnerships of mutual interest" (p. 61). The Kenya National ICT Masterplan – Towards a Digital Kenya (2014) outlines Kenya's efforts in participating in meetings at international platforms such as ICANN and ITU based on "shared principles, norms, rules, decision-making procedures, and programmes" (p. 17). Furthermore, the Masterplan highlights Kenya's endeavors and main concerns in implementing norms and regulations that are shaped through various international platforms embedded in common agreements and the involvement of multiple stakeholders. Thus, Kenya pursues a domestic CG approach which is authorized by the national government to legitimize the urge of establishing cyber security capabilities to enhance domestic security and social welfare (National Cybersecurity Strategy, 2014). Furthermore, The Computer Misuse and Cybercrimes Act (2018) "provide[s] for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention […] of computer and cybercrimes" to strengthen domestic security (p. 40). Hereby, the Kenyan National ICT Masterplan – Towards a Digital Kenya (2014) states Kenya's ambitions to "transitioning to a Knowledge Society and position the country as a regional ICT hub by developing quality ICT infrastructure"(p. 42). Furthermore, the Kenyan National Cybersecurity Strategy (2022) frequently mentions that in developing a stage of socialization in CG the government must foster the enhancement of cyber capabilities: "To ensure the availability of cutting-edge capabilities amidst rapid technology

change, the Kenyan government will support advanced research, local digital innovation, and develop local cybersecurity skills and knowledge to position Kenya as a continent leader in cybersecurity" (p. 12).

4.3. Norm internalization

Referring to Kenya's CG approach the stage of (3) *Norm internalization* and the subcategories of *laws, conformity, and institutionalization* are steered by the aim of regulating cyberspace on the domestic level. Therefore, Kenya attempts to internalize domestic cyber laws to enhance the infrastructure of CG and security adapted to international standards and regulations. Crucially, it addresses the urge to establish cyber security through privacy and data protection which is provided by the government's CG framework (Appendix 2) (National Cybersecurity Strategy, 2022). Furthermore, the National Cybersecurity Strategy (2022) emphasizes the importance of reaching conformity and norm compliance of the general public in setting the goals of educating Kenyan citizens to "take precautions to protect themselves and their valued possessions in the virtual world" (p. 5). Therefore, The National ICT Masterplan – Towards a Digital Kenya (2014) highlights the goal of enhancing the affordable access to ICTs for every citizen and "Implement awareness programs on the role of information and ICT for quality of life" (p. 53). As emphasized in the Masterplans and Strategy Papers, the Kenyan government follows the concerns of strengthening its domestic CG approach aiming to further set up CG bodies to "Establish a National Cybersecurity Operation Centre (NSCO)" and "co-operate with computer incident response teams and other relevant bodies, locally and internationally on response to threats of computer and cybercrime incidents" (National Cybersecurity Strategy, 2022, p. 8; The Computer Misuse and Cybercrimes Act, 2018, p. 47).

4.4. Development of cyber governance regulations over time

Analyzing and comparing the development of norm regulations in the period from 2014 until 2022 is crucial to indicate the shift in the agenda of CG. As aforementioned, the National Cybersecurity Strategy (2014) states Kenya's long-time goal of consolidating economic growth and the development of the application of ICTs to enhance the country's persuasion and image in global governance, especially in regulating cyberspace. Hereby, the National Cybersecurity Strategy indicates: "Kenya is committed to the safety, security, and prosperity of our nation" (p. 4). Furthermore, the Strategy frequently underscores the national goal to strengthen its cybersecurity strategy and national knowledge production which simultaneously must result in economic growth thereof. It highlights "cyber security as a key component

[…] encouraging greater foreign investment" (p. 4). In contrast, the National Cybersecurity Strategy (2022) set the goals of mutual collaboration and cooperation, especially on the regional and global level through multiple stakeholders, inter alia, the private and public sectors and businesses to address cyber threats. Therefore, the government promotes the development of a "national framework for national, regional and international co-operation and collaboration" to consolidate "Kenya's cybersecurity posture" (National Cybersecurity Strategy, 2022, p. 14). Furthermore, derived from the policy documents the findings demonstrate the formation of the CG targets over time. By emphasizing that "Kenyan data remains in Kenya" it is apparent that the country follows a domestic CG approach to securing data within its sovereign borders (The National Information and Communications and Technology (ICT) Guidelines, 2020). Thereby, the country intends to put local and national solutions, knowledge production, research, and policymaking over external influence which aligns with the Chinese model of CS (National ICT Policy Guidelines, 2020; The Kenya National ICT Masterplan – Towards a Digital Kenya, 2014). Moreover, the implementation of three CG Acts in 2018, 2019, and 2020 proclaim the commitment to enhance national security (Appendix 2). Internationally, Kenya documents in its Masterplans and Strategy papers the urge for law-making on common ground and acknowledges the "impact of cyberspace is accelerating across the national and international boundaries, making it a complex challenge for any government to address alone" (National Cybersecurity Strategy, 2014, p. 5). Hence, on the national level, Kenya's CG approach to the Chinese model of CS appears related. The Kenyan CG model consists of the coordination of cyber security bodies, counties, and ministries led by the national government that steers national law-making while simultaneously underscoring mutual cooperation and law-making through international platforms in the global arena which stands in contrast to the model of Chinese multilateralism. Furthermore, the policy documents demonstrate Kenya's endeavors to gain independence from external influential entities and achieve an "international image of Kenya as a digital economy able to offer appropriate digital support to other countries" (The Kenya National ICT Masterplan – Towards a Digital Kenya, 2014, p. 63).

5. Discussion

The discussion section intends to interpret the main findings of the QCA that are described in the analysis section and put them in a broader context of the scientific debate on GCG. Hereby, it tends to answer the research question as well as the related sub-question. The findings are linked to existing scientific literature, to Kenya's behavior in the global governance arena with reference to *sub-question (1)* and China's NP in promoting CS and multilateralism in linking it to *sub-question (2)*. Furthermore, unexpected

findings are discussed, their meaning interpreted in regard to the debate on (G)CG and the theoretical implications and contributions of the findings to the framework of the NLC indicated. Finally, a sufficient answer to the main research question is provided by outlining the degree of Chinese influence on Kenya's domestic regulatory framework and elaborating on the limitations of the research method and data collection.

5.1. Kenya's global cyber governance model

The main findings of the analysis that were examined through the lens of the NLC with a specific focus on China's norm entrepreneurship developed the understanding of Kenya ensuing to evolve into a crucial actor in GCG intertwined with the concern of economic growth. Referring to the three stages of the NLC in the instant of (1) *Norm emergence*, Kenya, as a sovereign state, attempts to influence GCG by participating in organizational platforms driven by the incentive of enhancing economic growth and obligating international agreements to consolidate its persuasive power in GCG regulation. In the stage of (2) *Norm cascade*, Kenya strives for mutual cooperation, law-making, and collaboration with multiple stakeholders through organizational platforms such as the ITU. Crucially, in underscoring the urge for enhancing persuasion Kenya struggles for the independency of external influence in domestic CG regulation and attempts consolidate its posture in decision-making at various international platforms. Interestingly, Kenya was recently elected as a member of the ITU council for the period from 2023- 2026 (including 12 other African nation-states). Hereby, as an ITU member Kenyan representatives are empowered to contribute to policy directions, decision making, and strategy settings. Frankly, it promotes collaboration and cooperation among stakeholders and enables Kenya to shape, recommend, and promote (1) *Norm emergence* and persuade decision-making in GCG that represents the national interest (International Telecommunication Union, 2022; ITU News, 2022). Certainly, as already mentioned before China profoundly utilizes the ITU as a platform and therefore also holds membership in the ITU council. In addition, the Secretary-General of the ITU was chaired by a Chinese representative for two terms but was recently replaced by a representative from the US. The Secretary-General is empowered to coordinate and lead the international telecommunication regulation in facilitating the development of global standards and guidelines. Crucially, it emphasizes that the two countries that tirelessly aim to influence the GCG debate are empowered to steer decision-making from top down. Nonetheless, their power is constrained by collective decision-making at the ITU council and leaves room for countries such as Kenya to contribute to (1) *Norm emergence* (International Telecommunication Union, 2018; 2023; Tugendhat &

Voo, 2021). Furthermore, Tugendhat & Voo (2021) display the participation of African countries in the ITU study group for Future Networks (SG13), in which China submitted up to 50 percent of the contributions and point out that Kenya solely contributed once. Generally, they highlight the rather narrow support for Chinese proposals by African DSR recipients. Besides that, the Kenyan policy documents list several memberships in organizational platforms such as ICANN. Since China rather opposes cooperation through ICANN, but it is extremely active at ITU it alludes to China's concept of multilateralism, the vigorous interest in promoting international co-governance through UN bodies and contesting the hegemonic stance of the US (Gao, 2022). Nonetheless, it is debatable whether China is able to directly influence the Kenyan domestic CG framework through the ITU. It rather refutes the Kenyan support for the Chinese model of CG in organizational platforms such as ITU.

5.2. Cyber sovereignty and multilateralism in the Kenyan context

Furthermore, taking China's model of CS and multilateralism into an account linked to Kenya's interest in developing into a powerful actor in the global arena led by the incentive of economic growth, it seems rather problematic, even fatal, to support and align with the concept of multilateralism. Crucially, derived from the policy documents Kenya set the national goals of economic development and social welfare embedded in CG through reaching conformity and socialization on the domestic level. Since Kenya strongly depends on foreign infrastructure investments and loans it cannot isolate itself from cooperating with multiple stakeholders, for instance, companies and the private sector, on the regional and global level since international economic cooperation goes in hand with diplomatic cooperation and collective decision-making (Rapanyane, 2021). Zheng & Di (2022) indicate developing countries, in this case, Kenya, "have realised the importance of cyberspace, the emerging global commons and accelerated the introduction of relevant policies to formulate cyberspace that conform their development and are in line with international standards" (p. 462). Even though the country heavily cooperates in infrastructure development with China, it does not simultaneously lead to the adaptation of the Chinese CG model of multilateralism due to Kenya pursuing a rather multi-faceted and multi-stakeholder approach of GCG which is elaborated on in the following.

5.2.1 China as a role model to gain economic growth?

In its National Cybersecurity Strategies (2014) and (2022) the Kenyan government states the goal of increasing economic growth while cooperating on the local, national, and international level with multiple

stakeholders, such as the public and private sector. Hence, the model of Chinese multilateralism appears to be barely (up to not at all) influential on Kenya's behavior in the global arena. In contrast, the concept of CS appears to be adapted on the national level. Frankly, this is not surprising in the sense that both nation-states desire to protect and secure their national data, and digital landscape, and claim sovereignty within their borders. Hereby, Kenya and China can be seen as equal players in the global arena which can be traced back to China's promotion of equality, peaceful cooperation, the principle of inclusiveness, and sovereignty in GCG. As aforementioned, Kenya legitimizes norm development and cascade based on the urge to enhance domestic security that is embedded in cyber security. Hereby, the Kenyan government acknowledges the need for expanding to a knowledge society and fostering national research and digital innovation. It indicates Kenya's efforts to strengthen the national knowledge infrastructure and cyber capabilities to uprise a crucial player in global cybersecurity. Thus, in theory, Kenya strives to decrease its dependency on cyber powers such as China but in practice, Kenya may imitate the Chinese trajectory of gaining independency from foreign technologies and economic autonomy. Hereby, the Kenyan government might admire China's powerful rise as a latecomer country and takes it as a role model in domestic cyber regulations (Yang et al., 2023). In addition, referring to the stage of (3) *Norm internalization* Kenya implemented three Acts that regulate cyberspace to address cyber insecurity on the domestic level (Appendix 2). Albeit, to reach sufficient and smooth norm internalization, Kenya states in its policy documents the establishment and rectification of CG bodies. Consisting of several entities and guided by the national government the structure of the Chinese and Kenyan landscape is seemingly alike (Creemers, 2021; National Cybersecurity Strategy, 2022). Crucially, taking the Chinese concept of CS into account Creemers (2021) and Gao (2022) unveil the (mainly) mistakenly framed determination of the Chinese centralized CG structure by Western countries. They emphasize that the concept of Chinese CS and the national governance approach, indeed, involves businesses contributing to regulating technical standards in CG. Hence, China's CS model is not solely steered by government authorities and a purely centralized concept but rather prevailed by divergent government bodies and public-private cooperation which "increases the possibility of a convergence between China's and Western countries' approaches to cyber governance" (Gao, 2022, p. 22). Therefore, Kenya's national CG framework and structure align with the Chinese model of CS due to similar concerns in norm regulations of data security and cybercrime acts. Hereby, China's persuasive and discursive power, which was elaborated on in the theory section, may play a key role in influencing the imitation of the CS model in Kenya domestically which seems a valid alternative to the US-centric model of CG (Gao, 2022; Chang, 2023). Chang (2023) indicates that "the China model can be broadly considered as a model of governance and development in which the state possesses

the strength and ability to mobilize society for the sake of prosperity, stability, and national security" which appears to be followed by the Kenyan national government (p. 12).

5.2.2. Economic cooperation as a facilitator of norm diffusion?

As aforementioned in the case description, Kenya heavily depends on foreign loans and infrastructure projects. Besides, Gagliardone (2019) highlights the cooperation between China and African countries neither results in a decrement in the democratization level nor does China actively promotes its media and telecommunication model and attempts to promote its political system abroad while providing assistance. Consequently, it delivers feasible insights into the mainly economic-based cooperation through the BRI/DSR in the case of Kenya (Gagliardone, 2019). The cooperation and participation in the BRI/DSR appear to be solely steered by the concerns of enhancing economic infrastructure development, prosperity, and growth even though Kenya is sliding into a 'Chinese debt trap' through the dependency on Chinese infrastructure projects and loans (Bensch, 2023). In short, this disproves the assumption that the DSR embedded in the BRI simultaneously affects the Kenyan domestic CG landscape. It contributes to the debate that China, despite its prevailing economic ties with African countries, specifically in this case Kenya, narrowly actively (re)shapes national regulation of its partner countries. Respectively, as mentioned earlier Kenya recently introduced three CG Acts to protect national cyberspace which puts the country in a position to avoid external influence in the matter of domestic CG and act independently (Appendix 2). Thus, Kenya does not follow the interest of strengthening its diplomatic ties and enhancing political exchange with China as with any other country. This disproves the fears of many Western countries, such as the US that China attempts to impose its political system abroad (Gagliardone, 2019). Thus, in the case of Kenya, bilateral economic cooperation as a factor that may enhance alignment with the Chinese CG model, does not lead to facilitating norm cascade and diffusion in Kenya.

5.2.3. Evolvement to a middle power following the EU model?

Thereby, indicating Kenya's distinctive behavior to the Chinese model of multilateralism in GCG is motivated by the concerns of exploiting all possible resources to play a crucial part in international relations. As Cheng & Yang (2022a) deal with the topic of global cyberspace regulation and the influence of powerful countries they highlight that the GCG debate is mostly discussed through the lens of the West vs non-west paradigm, namely China and Russia vs. the US and its Western allies. They contest this dichotomy by contextualizing the underrepresentation of rising 'middle power' states (in their case

Singapore and South Korea) and associations such as ASEAN and the European Union. Therefore, they emphasize the development of a global arena of "westlessness" and the rise of middle-power states that aim to emancipate from subordination and underrepresentation by the concepts of multilateralism and multistakeholderism in GCG. Kim (2022) utilizes the term middle power state in the context of South Korea and Singapore claiming independence from the predomination of the US-centric model of CG and the clash of West vs non-West. Their contextualization of GCG from a distinctive angle delivers valuable insights that are evident in the case of Kenya. Crucially, the concept of middle power states refers to Kenya's ambitions in the global arena to seemingly catch up, disentangle from external influence in CG regulation and arise to empower (Yang et al., 2023). Therefore, referring to Kenya's participation in organizational platforms, for instance, ITU and ICANN, indicates the endeavors to shape GCG decision-making that favors their national interest, to evolve into an NP and eventually a middle power country in following a "third way" in GCG (Cheng & Yang, 2022a, p. 11- 12). Hence, in taking Kenya's GCG approach into account, it could be alleged that the Kenyan government desires to align with the European cyber model which is shaped by data and digital sovereignty and greater government intervention than the model of the US (Gao, 2022). Crucially, the EU is categorized as a middle power player and its CG model is classified in between multilateralism and multistakeholderism (Chen & Yang, 2022b). Its regulatory CG framework is backed by the General Data Protection Regulation (GDPR) which incorporates universal values, a rights-embedded CG approach, and strict guidelines for transferring data to external entities. Furthermore, the EU "proactively encouraged third countries to adopt GDPR-like regulations and laws, and its regulatory approach has indeed proven attractive to numerous third countries" (Chen & Yang, 2022b, p. 56). Greenleaf & Cottier (2020) state that the Kenyan Data Protection Act (2019) is closely aligned with the GDPR of the EU. It reveals that Kenya may pursue a CG model that adapts to a certain degree with CS and the GDPR that elucidates its behavior in the global arena. Crucially, these are unexpected findings in referring to the research assumptions and research question, and sub-questions that still need further research to be supported.

5.3. Theoretical implications

In utilizing the theoretical framework by Finnemore & Sikkink (1998) it is identified that Kenya's behavior and interest in GCG are steered by economic incentives and security concerns. It emphasizes Kenya's active participation in international platforms through the interest of increasing its persuasive standpoint and influence in the process of (1) *Norm emergence.* Thus, Kenya is driven by the concerns of contributing to international law-making to shape norms that reach the tipping point favoring its national interest. As

Finnemore and Sikkink (1998) emphasize “Norms and rationality are thus intimately connected”. Arguably, the rational behavior of Kenya is shaped by the rational interest of norm evolvement in CG to benefit its economic growth and national security (p. 888). Hence, Kenya’s actions may be highlighted by striving for economic growth and emancipation albeit imitating the Chinese CS approach. Kenya’s national behavior is guided by leadership and CG regulation to consolidate its power in global governance and norm regulation. Finnemore & Sikkink (1998) emphasize the interconnectedness of domestic and international norms which explains the adaptation to CS on the national level through a strong domestic CG framework to generate a powerful stance in GCG. Therefore, it can be pointed out that economic growth and citizens’ well-being are crucial factors for international cooperation and conformity with international norms. It steers the behavior of economically weaker countries such as Kenya in participating to empower, increase economic growth as well as secure its (cyber) sovereignty in domestic law- and decision-making. Hereby, Finnemore & Sikkink (1998) indicate imitating the behavior of countries throughout the NLC is influenced by the “benefits of norm adherence” (p. 895). Thus, the term incentive is utilized as a subcategory under the domain motive indicated as a crucial factor that forms (1) *Norm emergence* (Figure 2). It emphasizes that incentives determine the behavior of actors in norm compliance and participation in organizational platforms and relations due to actively contributing to the norm and life cycle of laws and regulations in GCG. Furthermore, China’s norm entrepreneurship explained through the NLC can be stated as less influential in the case of multilateralism in Kenya, especially through organizational platforms. Therefore, China’s motives and dominant mechanism are not convincing in the Kenyan examples. However, the promotion of CS is supported to a greater extent.

5.3.1. Limitations

Even though the analysis delivered valuable insights limitations must be acknowledged. Crucially, the paper does not provide an answer to how the fragmentation in GCG may be addressed due to solely scrutinizing China’s norm entrepreneurship. The paper rather focuses on explaining the cycle of norm development promoted by China as NP in the specific case of Kenya to deliver a nuanced understanding of GCG implementation through international organization and bilateral cooperation. QCA is a sufficient method for identifying patterns and gaining an in-depth understanding of textual data. It nonetheless is constrained by limitations. Crucially, the textual analysis reflects and provides an in-depth meaning of the findings but does not analyze the occurrences of data which minimizes the reliability of the findings. As the analysis is mainly based on strategy papers, master plans, and annual reports the collected and code textual data rather demonstrate the goals and strategies that the Kenyan government aims to address

and regulate than scrutinizing internalized laws, regulations, and acts. This impacts the validity and contextual meaning of the findings. Furthermore, the theoretical framework of the NLC attempts to explain which and why laws promoted by NPs reach the tipping point and cascade. The structure of the thesis and the conducted coding scheme and the analysis do not provide explicit examples in respect thereof. The findings rather elucidate and elaborate on Kenya's behavior in the global arena of GCG regulation attempting to act independently albeit imitating Chinese CS domestically. Hence, the research findings do not provide evidence for specific norms (re)shaped by China's norm entrepreneurship that were internalized domestically.

6. Conclusion

In summarizing the main implications identified throughout this paper it provides sufficient findings on China's role as an NP and its CG models of CS and multilateralism, Kenya's domestic CG approach, and behavior in GCG regulation. Hence, the conducted QCA on China's NP analyzed through the theoretical framework of the NLC is able to deliver valuable insights to provide a sufficient answer to the research query and its sub-questions to a certain extent. Crucially, the literature review on the Chinese CG approach delivered fruitful insights into China heavily utilizing UN bodies, especially the ITU, as organizational platforms to promote equality, sovereignty, and co-governance as crucial factors embedded in its models of GCG. The case selection of Kenya was driven by scrutinizing a country that heavily cooperates with China in (digital) infrastructure projects that may contribute as a factor of facilitating adaptation to the Chinese model of CG for which was no evidence found in the policy documents. In answering the research question and its sub-questions, there are no significant findings that Kenya explicitly persecutes the Chinese model of multilateralism in the global arena. Nonetheless, the analysis of Kenyan policy documents emphasizes that the country imitates Chinese CS to a certain degree on the national level. Hence, China as an NP does not directly influence the national regulations, but Kenya rather imitates the Chinese approach alluding to aspiring after China's economic development as a latecomer state to a certain extent. It implicates the endeavors of securing national data and addressing cybercrimes independently. Therefore, participation in an international platform is a fundamental factor in enhancing persuasion in GCG due to a well-developed domestic regulatory framework may enhance its international stance in GCG and at international platforms such as ITU. Generally speaking, Kenya strikes as an example of a developing country striving for maturing into a crucial player in global governance through complying with and contributing to the norm regulation of GCG (Freedom House, 2023b). Hence, the findings guided by the NLC highlight that Kenya's behavior in the global arena is driven by the incentive of increasing

economic growth, societal welfare, and domestic security. Furthermore, the research on norm entrepreneurship in GCG in the case of Kenya provides the practical insights that China pursues promoting its CG model globally whereas Kenya is driven by the interest to consolidate its national concerns and evolve as a crucial player through a multifaceted (and multistakeholder) CG approach on the global level. Hereby, to put Kenya's GCG approach into a broader context of the scientific debate on GCG, Kenya may adapt to the cyberspace model of the EU in the global arena which needs further in-depth research to provide meaningful insights. Furthermore, the research implies that Kenya may attempt to transcend into a middle power country in GCG to disentangle from acting under the hegemonic authority of powerful countries such as the US and China which need additional investigation to be proven (Kim, 2022). In conclusion, to answer the main research question, the findings imply that Kenya does imitate the Chinese model of CS on the national level, which indicates that China's norm entrepreneurship promoted through international platforms does shape CG norm regulation and goal selection in Kenya to a certain extent.

7. References

Agbebi, M. (2022). China's Digital Silk Road and Africa's Technological Future. In *Council on Foreign Relations*. https://trepo.tuni.fi/handle/10024/138193

Bensch, K. (2023). *Kenia und Chinas Investitionen: Wie raus aus den Schulden?* Tagesschau. https://www.tagesschau.de/ausland/afrika/kenia-china-schulden-101.html

Chang, Y. Y. (2023). China beyond China, establishing a digital order with Chinese characteristics: China's growing discursive power and the Digital Silk Road. *Politics & Policy*, *00*, 1–39. https://doi.org/10.1111/POLP.12524

Chen, X., & Yang, Y. (2022a). Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness, *57*(3), 1–14. https://doi.org/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, *57*(3), 48–65. https://doi.org/10.1080/03932729.2022.2066841

Collins, C. S., & Stockton, C. M. (2019). The Central Role of Theory in Qualitative Research. *International Journal of Qualitative Methods*, *17*, 1–10. https://doi.org/10.1177/1609406918797475

The National Information and Communications and Technology (ICT) Guidelines, (2020) (testimony of Communications Authority of Kenya). https://www.ca.go.ke/wp-content/uploads/2020/10/National-ICT-Policy-Guidelines-2020.pdf

Annual Report, Fostering Digital Transformation through Building a Connected Society, Enabling Regulation, Partnership and Innovation, (2021) (testimony of Communications Authority of Kenya). https://www.ca.go.ke/search/node?keys=Annual+Report%2C+Fostering+Digital+Transformation+through+Building+a+Connected+Society%2C+Enabling+Regulation

Creemers, R. (2021). *China's Cyber Governance Institutions*. https://leidenasiacentre.nl/wp-content/uploads/2021/01/Chinas-Cyber-Governance-Institutions-Layout-geconverteerd-1.pdf

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/J.1365-2648.2007.04569.X

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, *52*(4), 887–917. https://doi.org/10.1162/002081898550789

Finnemore, M., & Sikkink, K. (1998). *Norm Life Cycle* [Graphic]. International Norm Dynamics and Political Change. International Organization, 52(4), 887–917. https://doi.org/10.1162/002081898550789

Finnemore, M., & Sikkink, K. (1998). *Stages of norms* [Table]. International Norm Dynamics and Political Change. International Organization, 52(4), 887–917. https://doi.org/10.1162/002081898550789

Freedom House. (2023a). *Freedom in the World 2023 China*. https://freedomhouse.org/country/china/freedom-world/2023

Freedom House. (2023b). *Freedom in the World 2023 Kenya*. https://freedomhouse.org/country/kenya/freedom-world/2023

Gagliardone, I. (2019). China, Africa, and the Future of the Internet. In *China, Africa, and the Future of the Internet*. Zed Books Ltd. https://doi.org/10.5040/9781350219113

Gagliardone, I., & Sambuli, N. (2015). *Cyber Security and Cyber Resilience in East Africa - Centre for International Governance Innovation*. https://www.cigionline.org/publications/cyber-security-and-cyber-resilience-east-africa/

Gao, X. (2022). An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. *International Spectator*, *57*(3), 15–30. https://doi.org/10.1080/03932729.2022.2074710

Given, L. M. (2008). The SAGE Encyclopedia of Qualitative Research Methods. In K. Saumure (Ed.), *SAGE Publications* (Vols. 1 & 2, pp. 1–1014). https://books.google.nl/books?hl=de&lr=&id=byh1AwAAQBAJ&oi=fnd&pg=PP1&dq=given+2008&ots=LPX-ON2M5u&sig=zjzRTfwlP1RDwpIL-eZh5G1bejE&redir_esc=y#v=onepage&q=given%202008&f=false

Glen, C. M. (2021). Norm Entrepreneurship in Global Cybersecurity. *Politics & Policy*, *49*(5). https://doi.org/10.1111/polp.12430

Greenleaf, G., & Cottier, B. (2020). Comparing African Data Privacy Laws: International, African and Regional Commitments. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3582478

Hurel, L. M. (2022). Interrogating the Cybersecurity Development Agenda: A Critical Reflection, *57*(3), 66–84. https://doi.org/10.1080/03932729.2022.2095824

The Kenya National ICT Masterplan - Towards a Digital Kenya, (2014) (testimony of ICT Authority of Kenya). https://www.ict.go.ke/wp-content/uploads/2016/04/The-National-ICT-Masterplan.pdf

International Telecommunication Union. (2018). *ITU Member States re-elect Houlin Zhao as ITU Secretary-General*. https://www.itu.int/en/mediacentre/Pages/2018-PR35.aspx

International Telecommunication Union. (2020). *Global Cybersecurity Index - Measuring the commitment to cybersecurity*.

International Telecommunication Union. (2022). *ITU Council*. https://www.itu.int/en/council/2022/Pages/default.aspx

International Telecommunication Union. (2023). *Office of the Secretary-General*. https://www.itu.int/en/osg/Pages/default.aspx

ITU News. (2022). *Elections completed for ITU Council and Radio Regulations Board*. https://www.itu.int/hub/2022/10/elections-results-itu-council-radio-regulations-board-pp22/

Kim, S. (2022). Roles and Limitations of Middle Powers in Shaping Global Cyber Governance. *Https://Doi.Org/10.1080/03932729.2022.2097807*, *57*(3), 31–47. https://doi.org/10.1080/03932729.2022.2097807

Krippendorff, K. (2004). Reliability in content analysis: Some misconceptions and recommendations. *Human Communication Research*, *30*(3), 411–433. https://doi.org/10.1111/J.1468-2958.2004.TB00738.X

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, *30*.

LY, B. (2020). Challenge and perspective for Digital Silk Road. *Http://Www.Editorialmanager.Com/Cogentbusiness*, *7*(1), 1804180. https://doi.org/10.1080/23311975.2020.1804180

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security*. www.gppi.net

McBride, J., Berman, N., & Chatzky, A. (2023). *China's Massive Belt and Road Initiative*. Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Ministry of Foreign Affairs of the People's Republic of China. (2021). *China's Positions on International Rules-making in Cyberspace*. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html

Ministry of Foreign Affairs of the People's Republic of China. (2023). *Strategy for International Cooperation in Cyberspace*. https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/201703/t20170301_7669140.shtml

Omolo, M. D., Wanja, R., & Jairo, S. (2016). Comparative Study of Kenya, US, EU and China Trade and Investment Relations. *Institute of Economic Affairs*.

https://www.africaportal.org/publications/comparative-study-kenya-us-eu-and-china-trade-and-investment-relations/
Pratt, M. K. (2019). ICT (information and communications technology, or technologies). CIO. https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies
Rapanyane, M. B. (2021). Neocolonialism and New imperialism: Unpacking the Real Story of China's Africa Engagement in Angola, Kenya, and Zambia. *Journal of African Foreign Affairs*, *8*(3), 89–112. https://journals.co.za/doi/abs/10.31920/2056-5658/2021/v8n3a5
National Cybersecurity Strategy, (2014) (testimony of Ministry of Information Communications and Technology). https://www.ict.go.ke/downloads/NATIONAL%20CYBERSECURITY%20STRATEGY%20HIGH.pdf
The Computer Misuse and Cybercrimes Act, (2018) (testimony of Republic of Kenya). https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/
National Cybersecurity Strategy, (2022) (testimony of Republic of Kenya). https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/
Saldana, J. (2016). An Introduction to Codes and Coding. In *The Coding Manual for Qualitative Researchers* (3rd ed.). Sage. https://www.sfu.ca/~palys/Saldana-CodingManualForQualResearch-IntroToCodes&Coding.pdf
Savas, S., & Karatas, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *Law Rev*, *3*, 7–34. https://doi.org/10.1365/s43439-021-00045-4
Tugendhat, H., & Voo, J. (2021). China's Digital Silk Road in Africa and the Future of Internet Governance. *School of Advanced International Studies*, *50*. http://hdl.handle.net/10419/248178
Yang, Y. hong, Gao, P., & Zhou, H. (2023). Understanding the evolution of China's standardization policy system. *Telecommunications Policy*, *47*(2), 102478. https://doi.org/10.1016/J.TELPOL.2022.102478
Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics and Policy*, *45*(3), 432–464. https://doi.org/10.1111/POLP.12202
Zheng, F. U., & Di, G. (2022). Global Cyber Governance in China: Towards Building a Community of Shared Future in Cyberspace. *Sage Publications*. https://doi.org/10.1177/09717218221075958

8. Appendix

Appendix 1

Concepts of cyber sovereignty and multilateralism

Concept	Author	Occurrence
Cyber Sovereignty	Chang (2023), Zeng et al. (2017), Tugendhat & Voo (2021), Glen (2021), Zheng & Di (2022), Gao (2022), Gagliardone (2019)	7
Multilateralism	Chang (2023), Zeng et al. (2017), Ly (2020), Tugendhat & Voo (2021), Zheng & Di (2022), Gao (2022), Cheng & Yang (2022a), Kim (2022), Gagliardone (2019)	9

Appendix 2

National cyber governance Acts

Year	Title	Description
2018	The Computer Misuse and Cyber Crimes Act	"AN ACT of Parliament to provide for offences relating to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with cybercrime matters; and for connected purposes" (National Computer and Cybercrimes Coordination Committee, 2018, p. 40)
2019	The Data Protection Act	"AN ACT of Parliament to give effect to Article 31 (c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes" (Communications Authority of Kenya, 2019, p. 905)
2020	The Kenya Information and Communications Act	"An Act of Parliament to provide for the establishment of the Communications Commission of Kenya, to facilitate the development of the information and communications sector (including broadcasting, multimedia, telecommunications and postal services) and electronic commerce, to provide for the transfer of the functions, powers, assets and liabilities of the Kenya Posts and Telecommunication Corporation to the Commission, the Telcom Kenya Limited and the Postal Corporation of Kenya, and for connected purposes" (Communications Authority of Kenya, 2020, p. 9)

Appendix 3

Policy documents analyzed

Year	Author	Title	Number of pages
2014	Ministry of Information, Communications, and Technology	The Kenya National ICT Masterplan – Towards a Digital Kenya	149
2014	Ministry of Information Communications and Technology	National Cybersecurity Strategy	24
2020	Communication Authority of Kenya	The National Information Communications and Technology (ICT) Policy Guidelines	17
2021	Communications Authority Kenya	Annual report- Fostering digital transformation through building a connected society, enabling regulation, partnership, and innovation	71
2022	National Computer and Cybercrimes Coordination Committee	National Cybersecurity Strategy	29

Appendix 4

Coding scheme

Category	**Kenya**		
	Subcategory	Definition	Example
Norm Emergence	*Entrepreneurship*	Participation in international platforms to *articulate stance* in GCG	*"The Kenyan Government is committed to work with international stakeholders such as academia, research institutions and private sector as well as international partners to improve Kenya's cybersecurity posture" (National Cybersecurity Strategy, 2022, p. 10)*
	Incentive	Cyber governance as an enabler of *economic growth*	*"The government of Kenya considers securing its national cyberspace a national priority to continue to facilitate economic growth for the country and its citizens" (National Cybersecurity Strategy, 2014, p. 5)*
	Persuasion	*Obligate* international agreements to *influence* GCG regulations	*"Active member of the International Telecommunications Union (ITU)" and "Enhance the international image of Kenya as a digital economy" (The Kenya National ICT Masterplan – Towards a Digital Kenya, 2014, p. 17)*
Norm Cascade	*International organization*	*Cooperation* with *multiple stakeholders* to enhance law-making on a common ground	*"Strengthening engagment and collaboration with all stakeholders to develop mechanisms and policies, and implement cybersecurity initiatives […] at national and international levels" (National Cybersecurity Strategy, 2022, p. 14)*

	Legitimacy	Enhancement of *domestic security* through cyber security	*"The Government of Kenya is taking steps to increase the security and resilience of its critical information infrastructure to protect its government, citizens and residents, and corporations from cyber threats" (National Cybersecurity Strategy, 2014, p.11)*
	Socialization	Foster *national research* and *cyber capabilities* to enhance cyber security	*"Ensure the availability of cutting-edge capabilities amidst rapid technology change, the Kenyan Government will support advanced research, foster local digital innovation, and develop local cybersecurity skills "(National Cybersecurity Strategy, 2022, p. 12)*
Norm Internalization	*Law*	Domestic regulation of cyberspace to enhance *national* and *citizens' security*	*"Review cybersecurity policies, laws, regulations and standards. Amend/update cybersecurity policies, laws, regulations, and standards." (National Cybersecurity Strategy, 2022, p. 9)*
	Conformity	*The public* must *adapt to and believe in the urge* to address cyber insecurity	*"Kenyan citizens and non-citizens must take precautions to protect themselves and their valued possessions in the virtual world" (National Cybersecurity Strategy, 2022, p. 5)*
	Institutionalization	Establishment of governance bodies to address *domestic cyber governance regulation*	*"Co-operate with computer incident response teams and other relevant bodies, locally and internationally on response to threats of computer and cybercrime and incidents" (The Computer Misuse and Cybercrimes Act, 2018, p. 47)*