AALBORG UNIVERSITET

Political Investigation into Sino-Tanzanian ICT Cooperation: Applying (De)Securitization Theory

Shujaa Benson

Study No. 20192577

Aalborg University

Master's Thesis

Characters: 105501

Development and International Relations

Faculty of Social Sciences

Date of submission: 31.01.2022

Abstract

The current thesis investigates the aspects of economic growth in the context of East Africa that have been largely left out of the research focus – the interconnection between the growth in the ICT field and Chinese influence in the region. Using the case study of Tanzanian ICT infrastructure and ICT-facilitated development projects, the current thesis aims at expanding the understanding of the linkage between these areas and Chinese growing influence in the region.

Securitization theoretical framework is employed in attempt to theorize the Sino-Tanzanian ICT partnership. Building upon the extensive review of the theoretical framework (Tanzanian context, securitization and desecuritization theories and their application to cybersecurity), we identify aspects of this partnership through the lens of security issues. By conducting a series of interviews with the Tanzanian ICT sector representatives, entrepreneurs, we explore the recurring themes and concerns the sector is facing on the path of further digital transformation and closer ties between the countries.

Findings of the thesis suggest technology transfer and capacity building as a key desecuritization path in the context of Tanzanian ICT, and that de-securitizing and de-politicizing concerns over over-dependence on external developmental aid. The idiosyncrasies of desecuritizing cyber-space are reflected as well as the opportunities of applying Securitization framework in African context is expanded in this thesis.

***Keywords**: ICT growth, growth patterns, securitization, desecuritization*

Contents

1. Introduction and Literature Review

1.1 Problem Statement

The *unprecedented expansion of the Chinese ICT sector across the developing countries,* specifically in Africa, has gained considerable media attention over the last years. Nevertheless, this area remains under-theorized with limited application of comprehensive research frameworks to study the phenomena. This is largely due to politicization of the discourse, with the global superpowers underlying *either positive or negative consequences of this cooperation.* This is also due to the perception of *inevitability of the Chinese* ICT internationalization considering that the China's ICT services production and export of ICT services doubled over the last decade (Hausmann, 2020) and that Chinese ICT products and services have a significant price advantage in the global markets.

In parallel to this trend, the geopolitical landscape and its "rules of the game" have undergone tangible transformation in the era of digitalization. Digital technologies per se changed the methods of exerting political influence since information and data become important political and economic resources. From data manipulations, elections meddling, power outages to tweaking algorithms, leakages of phone calls and social media content, there are numerous examples where data (mis)management was used to influence the political processes domestically and internationally. Moreover, digital transformation across developing countries leads to the fact that operations across longer spectrum of socioeconomic domains rely on information technologies. In this light, the limited range of large-scale ICT corporations, also referred to as "Big Tech", get to accumulate leverages over different aspects of economic and political development (Wong, 2021). While in developed countries, in many cases, it is hard to imagine any aspects of public or private sector operations that are non-digitalized, in the developing countries, this process is much slower and is inhibited by reliance on foreign capacity and investments, lack of digital literacy, and rudimentary levels of legislative frameworks in the ICT domain. On top of the sectors of socio-political and economic life that are conventionally considered "strategic" and as "related to national security" (military, energy sectors), we can argue that ***ICT sector at large, and ICT infrastructure sector particularly has become one of the Strategic Areas and key fields of national security, and is coming to the forefront of it.***

Tanzania represents a compelling case study to delve into these issues considering the number of factors. This country has been long considered a gateway of China into the African continent considering the longest history of infrastructure cooperation, which stem back in 1960s, and as it is one of the first developing countries to support the Chinese government diplomatically during the Cold War. Moreover, the dynamics of ICT development, where the central government plays a huge role by centralizing technological operational and regulatory framework as well as outlining very ambitious plans when it comes to digital transformation while remaining one of the most under-developed countries on the continent.

Despite the fact that the proliferation of Chinese development aid and ICT infrastructure projects across East Africa over the last decade has turned into a geopolitical matter much discussed in mainstream media, there is ***a lack of conceptualization in this field leaving an opportunity for further research.*** In this research, we are aiming at embedding the context of Sino-Tanzanian cooperation in the key ICT areas into well-established conceptual frameworks of securitization and desecuritization processes.

By employing the **(de)securitization theoretical framework** employed by the Copenhagen School of International Relations (Buzan et al., 1998; Balzacq, 2011; Nyman, 2013; Waever, 1993) and recent attempts to re-align this theoretical framework to the matters of cyber security (Cavelty, 2020; Hansen & Nissenbaum, 2009) and to contextualize it outside the Western perspective (Bilgin, 2011, Wilkinson, 2007, Ezeakafor & Kaunert, 2018), we are pursuing the following **research questions;**

1- Explore security concerns embedded into Sino-Tanzanian ICT cooperation, their magnitude and key components.

- Sub-question 1.1: Outline components of securitization framework (existential threat, securitizing actor, audience, emergency action, rhetorical devices, desecuritization paths)

2- Explore how these concerns are managed (securitized/desecuritized), and outline opportunities for desecuritization.

- Sub-question 2.1: whether ICT can be subjected to securitization at the early stage of development
- Sub-question 2.2: whether securitization framework as developed by the Copenhagen School of International Relations applicable “as-is” to the East African context

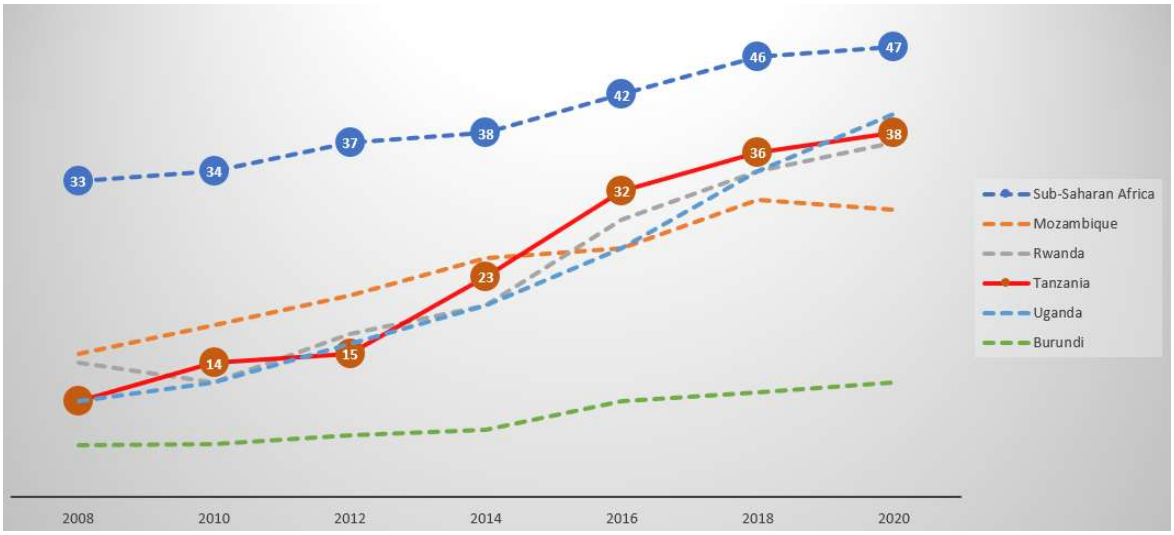
To address these research questions, our research is organized in the number of stages. First, we start our research with providing the context by examining closely the dynamics and preconditions of the ICT development in Tanzania, and the dynamics of Sino-Tanzanian partnership in this area and beyond. Second, we review the theoretical framework of securitization and desecuritization and reconnect it to the matters of cyber security and ICT development. Third, we employ the narrative and thematic analysis of the survey results to identify the contours of (de)securitization components within the Sino-Tanzanian ICT development. We further rely on these findings to identify possible paths for desecuritization that would enable mutually beneficial, secure, and growth-enabling ICT development patterns in Tanzania.

1.2 ICT Development in Tanzania: Preconditions and Historical Overview

Historical development of the ICT in Tanzania cannot be detached from the context of socioeconomic development. Still one of the least developed countries in Africa, Tanzania was lagging behind all the countries in the East African region by the mid-2010s, when both expansion of gold mining and rapid post-industrialization propelled by the tourism industry enabled Tanzania to achieve higher rates of GDP growth than regional average. In the period 2012-2018, Tanzania had an average GDP growth of 6.8%, which placed the country in the top 10 of the fastest growing economies in the world (The World Bank, 2021a). Gross National Income per capita almost doubled in the period between 2009 and 2019, from 599 USD to 1100 USD, respectively, which is higher than that in neighboring Mozambique, Rwanda, and Uganda (Gupta, 2020). *Low purchasing power* and high level of absolute poverty are fundamental factors that should be taken into account when analyzing the state of ICT development (Esselaar & Adam, 2013).

Another baseline factor is *electrification,* the indicator by which Tanzania remains one of the least developed countries in the world with 37.8% of the total population having access to grid electricity (The World Bank, 2021b). In line with the GDP growth, Tanzania experienced the drastic increase in electrification since the mid-2010s, being next only to Somalia in the level of the electrification growth rate in the world per year (IEA, 2021). Nevertheless, the country is still

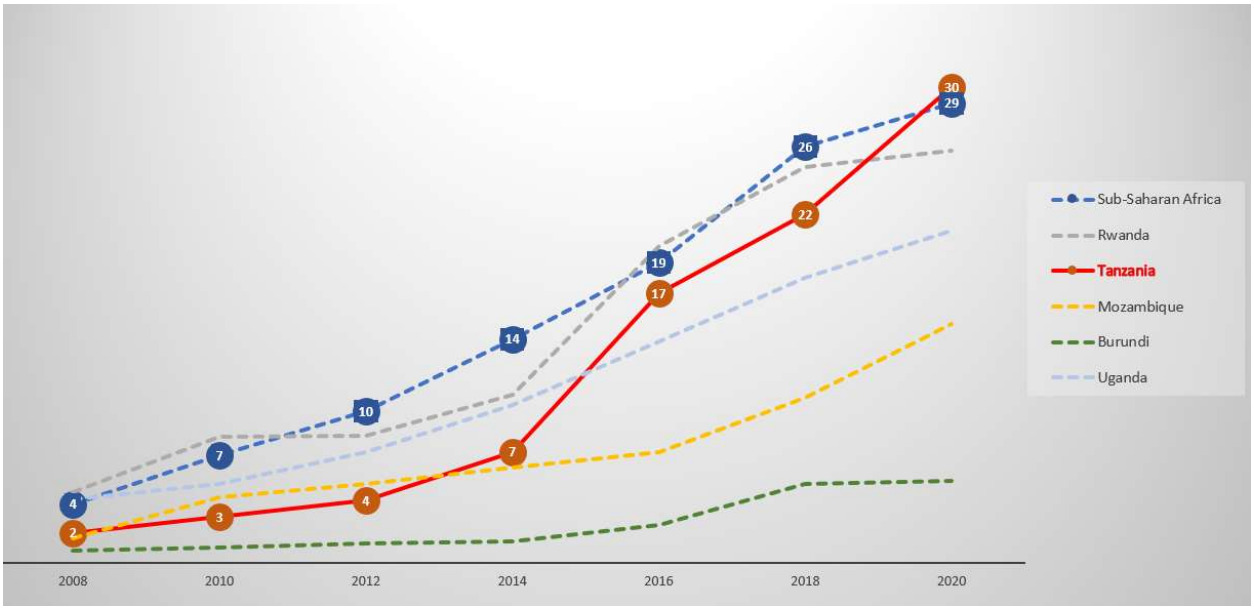
behind the Sub-Saharan Africa region average, which indicates the initial stage of electrification of the country (See Graph 1).



Graph 1. Access to Grid Electricity.

Data Source: The World Bank (2021b)

Access of electricity and household income determined low levels of mobile and broadband internet penetration. As of December 2020, 29.8% of the country's population access the internet daily (Graph 2), while the reach of the internet coverage reached 50% of the country's population (DataReportal, 2021). Smartphones and other portable devices account for 94% of the internet traffic generated in the country, and the high prices on smartphones determine the gap between the access to internet and coverage rates. At the same time, in terms of the internet coverage, Tanzania has experienced exponential growth over the last few years, where the number of population covered by internet/broadband services doubled in 2017-2020 and now exceeds 51% of the country's population, placing the country far above the regional average (Tanzania Communications Regulatory Authority, 2021).



Graph 2. Individuals daily accessing Internet (% of total population)

Data Source: The World Bank (2021c), IEA (2021)

The exponential growth that distinguished Tanzania from other countries in the region has taken place at the backdrop of the number of developments and strategic initiatives, which include:

1. *The National ICT Broadband Backbone (NICTBB),* which is the government-backed project of backbone fiber infrastructure rollout, including over 7500 km of fiber construction connecting the major cities of the country: Dar es Salaam, Dodoma, Morogoro, Mwanza and Arusha (Esselaar & Adam, 2013; Okeleke, 2018; UNCTAD, 2020). The project kick-started the broadband rollout in the country and enabled localization of the services. The National ICT Broadband Backbone project also significant reduction in wholesale rates by elimination of the duplicate networks, decreasing total broadband prices by more than 30% and the broadband rollout costs by 25% (Esselaar & Adam, 2013; Hoffman, 2018).
2. *High-Capacity International Submarine Cable Projects* boosted adoption of broadband services and connectivity of the country. First international projects, SEACOM and EASSY, which connected Tanzania with Seychelles, India, and East African countries were launched in 2010. Launch of these projects allowed the country to drift away from the path of using expensive satellite technologies towards cost-efficient network development. Since then, the Tanzanian government opted for becoming part of the

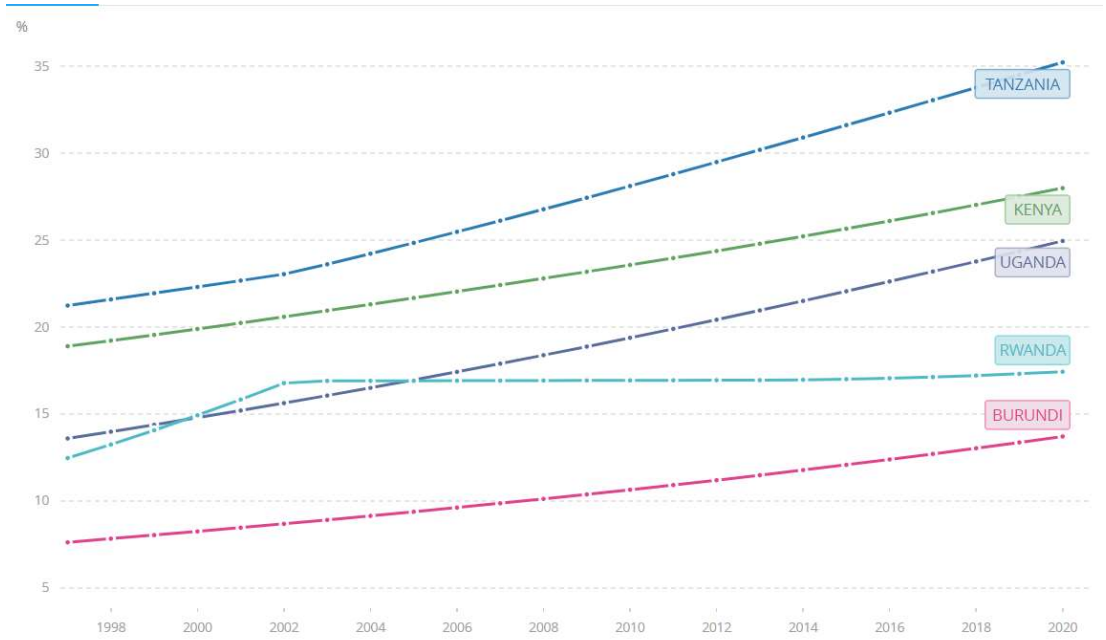
series of international initiatives for submarine connectivity such as connection between West Africa and East Africa by Liquid Telecom (Hoffman, 2018).

3. *Increased Competition and New Entrants on the Market.* Mobile network operators, still the largest contributors to the technological growth of Tanzania, represent a highly competitive environment with 8 major players, which contrasts to other countries in the region, where the market is split between 2-3 international holdings. The competition has driven down the mobile internet and mobile and fixed subscription prices and even enabled emergence of the MVNO market (UNCTAD 2020). The price of 0.5 GB mobile internet package today is less than 2 USD, less than two per cent of monthly GNI. Compared to other East African countries, the Tanzanian telecommunications market stands out by the absence of government-owned large corporations with the telecommunication regulator only playing the role of the broadband backbone operator (Johnson, 2018).

Mobile network proliferation through these projects enabled moving the economy past rudimentary technological development and created a range of favorable preconditions for positioning Tanzania as a regional technological hub. To reinforce the role of submarine connectivity in the leap forward made by Tanzania, it is enough to compare country's progress with that of its landlocked neighbors – Rwanda and Burundi, countries which have to rely on extension of the submarine cable through Tanzania's National ICT Broadband Backbone (UNCTAD, 2020).

Moreover, higher urbanization rates in relation to other low-income African countries fueled the faster internet adoption. With a divergently rapid growth in urban population from the mid-2000s, Tanzania reached the Sub-Saharan average level of urbanization of 36% in 2020 (The World Bank, 2021c) (Graph 3). Greater size and share of urban population are the reasons why more international network operators and telecom equipment providers invested in the country in comparison to the neighboring countries – Vodacom, Alcatel, Huawei, Millicom, as urbanization remains prerequisite for efficient wireless radio planning of network and minimizing rollout costs (UNCTAD, 2020). Exacerbated urban-rural digital divide became at the same time the major challenge for Tanzania to make faster digital transformation and de-fragmentize the

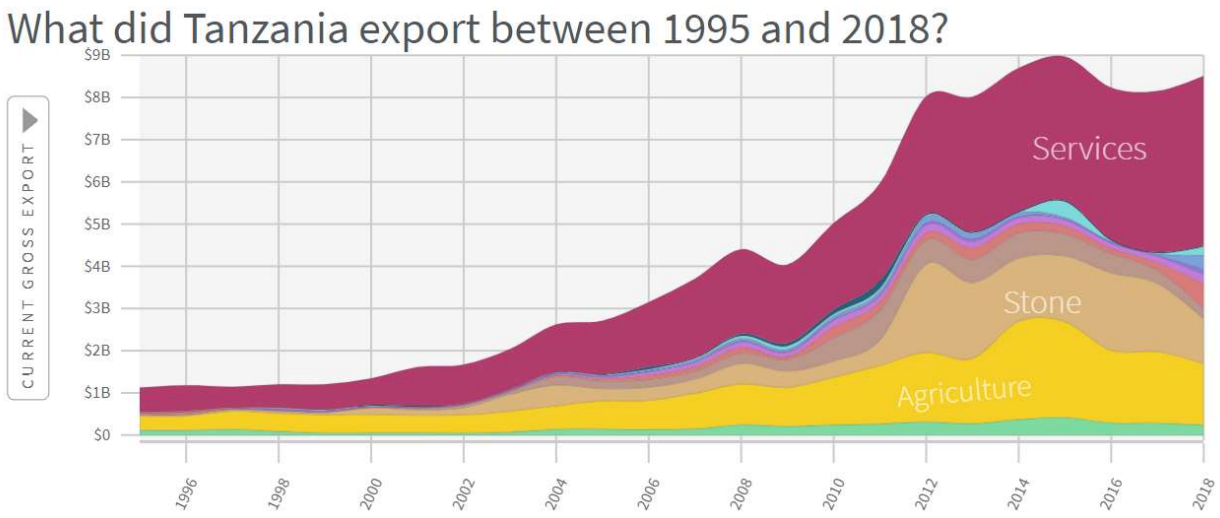
ICT sector. The Survey by the University of Dodoma revealed that there is almost two-fold gap in internet connectivity between rural and urban areas of Tanzania, underlying the fact that the mobile network operators are unwilling to invest in sparsely populated areas (UNCTAD, 2020).



Graph 3. East African Countries: Urbanization Rate, 1998-2020.

DataSource: The World Bank (2021)

The rates of post-industrialization, reallocation of resources to the services sector, in Tanzania has been among the most rapid in the world. Post-industrialization has particularly accelerated in the country from the beginning of the last decade, with the rapid expansion of tourism and ICT growth being the largest contributors to this process. The share of the services sector in the export portfolio of the country has grown from 28% in 2012 to 48.9% in 2020 (Hausmann, 2020; Mpambije, 2021). ICT-enabled businesses are the major contributors of the boosted exports in the major sectors of economy including tourism and agricultural, while ICT-specializing businesses account for a small (0.8%) share of export portfolio due to the concentration of the sector's resources in foreign-owned network operators (Graph 4).



Graph 4. Tanzania's export portfolio over time.

DataSource: ATLAS of Economic Complexity (Hausmann 2020)

Mobile network rollout plays a central role for the ICT development of Tanzania, which is also evident in the differentiation of usage of different information and communication technologies (Network Readiness Index, 2021). Nevertheless, the number of *challenges hindered Tanzania from achieving the level of adoption commensurate with the middle-income African countries*. According to Okeleke (2018), Tanzania was not able to fully exploit the benefits of the infrastructure projects and lowered broadband prices due to another market – smartphones and portable devices. As noted above, ca. 94% of Tanzanians have access to the internet via smartphones, yet smartphones remain unaffordable for the large share of population, particularly in rural areas. University of Dodoma survey (Okeleke, 2018) revealed that almost 2/3 of the population indicate that the high cost of smartphones is a hindrance to their usage of the internet. To address this obstacle, the Tanzanian Communications Regulatory Authority sought opportunities to attract foreign direct investments to build a smartphone factory in Tanzania involving public-private partnership arrangement (despite the number of government tenders, no specific agreements are reached to realize the project yet) (Parks & Thompson, 2020). The body of literature analyzing the relative success of ICT in Kenya emphasizes the existence of the sustainable and cost-effective smartphone factory as a key factor fueling its growth (Ndungu'u, 2019).

Another challenge is that the non-ICT-specializing private sector of Tanzania is characterized by lower adaptation to the digital transformation as well as government initiatives and regulatory changes. In many cases some regulations and laws that were adopted were ahead of time (UNCTAD, 2020) and led to collisions slowing the growth of business digital transformation. In 2018, Tanzanian Communication Regulatory Authority and Work Ministry implemented a new online content regulation, which presumes licensing requirements for publication of online content. Among other aspects, this regulates website development and web-blogging, which are subject to review and renewal by the regulatory authority (UNCTAD, 2020). This significantly limits SMEs in investing into front-end development, which is supported by low adoption of websites and knowledge management infrastructure (Tanzania ranks below all East African countries in this indicator) (UNCTAD, 2020). While the ICT environment in Tanzania is characterized by the high level of trust in governance and regulation, the private sector has shown the lack of participation in the initiatives (Okeleke, 2018).

To summarize the stage of ICT infrastructure and environment in Tanzania, we refer to the findings of the World Economic Forum's *Network Readiness Index* — the composite indicator that measures the application and the quality of information and communication technologies (Dutta & Lanvin, 2019; Sitnicki & Netreba, 2020). This index is selected for the purpose of characterization of the ICT environment since, in contrast to other assessment indices and global rankings, the Network Readiness Index (NRI) assigns particular emphasis to the *potential* of success of the country's environment in the digital economy rather than existing usage and preparedness of resources (Network Readiness Index Report, 2021). This represents a more suitable approach for the purpose of this study rather than using other indicators based on conventional measures of network proliferation and traffic. Moreover, NRI assessment embeds interconnection between different ICT development variables. In conventional development indices, the indicators on the quantity and quality of adoption of technologies (network penetration, coverage, access to internet etc.) are measured as analytically equivalent to indicators measuring Enabling Factors (capacity and knowledge management, network policies and regulations, etc.). This is addressed in NRI's methodology, where the relationship between these two groups is balanced, with the number of reports indicating that the index is more

effective in capturing the potential of communities' readaptation or "preparedness for the digital future" (Network Readiness Index Report, 2021).

Comparing to neighboring countries with a similar level of GDP and network penetration, it should be first noted that prior to mid-2000s, Tanzania was lagging behind all of the countries in the region except for Burundi (NRI ranking for Tanzania in 2013 was 112, for Uganda – 105, for Mozambique -104, and for Rwanda -99). Within a 4-year period between 2015 and 2019, Tanzania overtook its neighboring countries on many components.

Tanzania scores relatively high in the ***Governance*** component. The Tanzanian's Government's preparedness for the digital future is ranked as much higher than that for individuals and businesses in the country. This is based upon the strategic initiatives (such as NICTBB and international submarine cable networks discussed above) and visionary approach towards ICT adoption (Digital Tanzania Project plans, which outline the strategic development for each 5-year period ensure higher predictability and future-orientation of the economic modernization). High score on "Governance" Indicator is also ascribed to quiet early interest of the government in adoption of the ICT-enabled public services, such as e-governance and government online services.

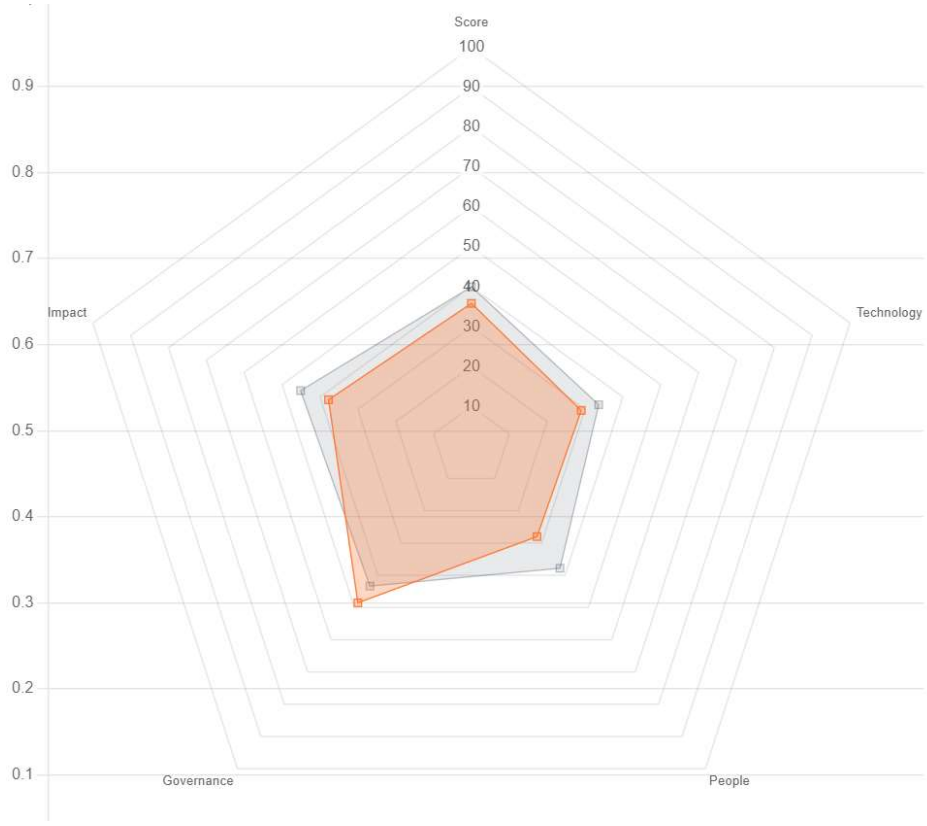
NRI	Score	Technology	People	Governance	Impact
Rwanda	38.65	29.03	34.94	47.58	43.03
Tanzania	35.83	29.03	28.03	48.55	37.74
Uganda	31.51	22.55	24.88	45.7	32.9
Mozambique	26.55	21.93	25.68	31.71	26.86
Burundi	22.48	18.86	23.37	20.85	26.85

Table 1. NRI Components. Tanzania and Neighboring Low-Income Countries.

Data Source: NetworkReadinessIndex.Org

Reviewing the findings of the World Economic Forum's report and Network Readiness Index Ranking,3 major strengths of Tanzanian ICT environment stand out not only from other indicators for Tanzania but from the overall mix of performance indicators in Sub-Saharan Africa;

- **Privacy protection by law content –** Tanzania is ranked #8 in the world in terms of this indicator due to the stringent framework around online content publications (described above).
- **Online access to financial institutions –** the rollout of the holistic mobile banking system in cooperation between the mobile network operators, Tanzanian government and Huawei ensured easy access to financial information by individuals and businesses.
- **Cybersecurity** – Tanzania is ranked #45 and #2 in Africa in terms of cybersecurity despite the lack of systemic legislative approach in this area but mostly due to early adoption of advanced digital encryption methods, know-your-customer methods implemented by the mobile network operators (Okeleke, 2018) and ICT-enabled government services (Network Readiness Index Report, 2021).



Graph 5. Network Readiness Index Ranking. Tanzania (red) vs Low-Middle-Income Group (blue)

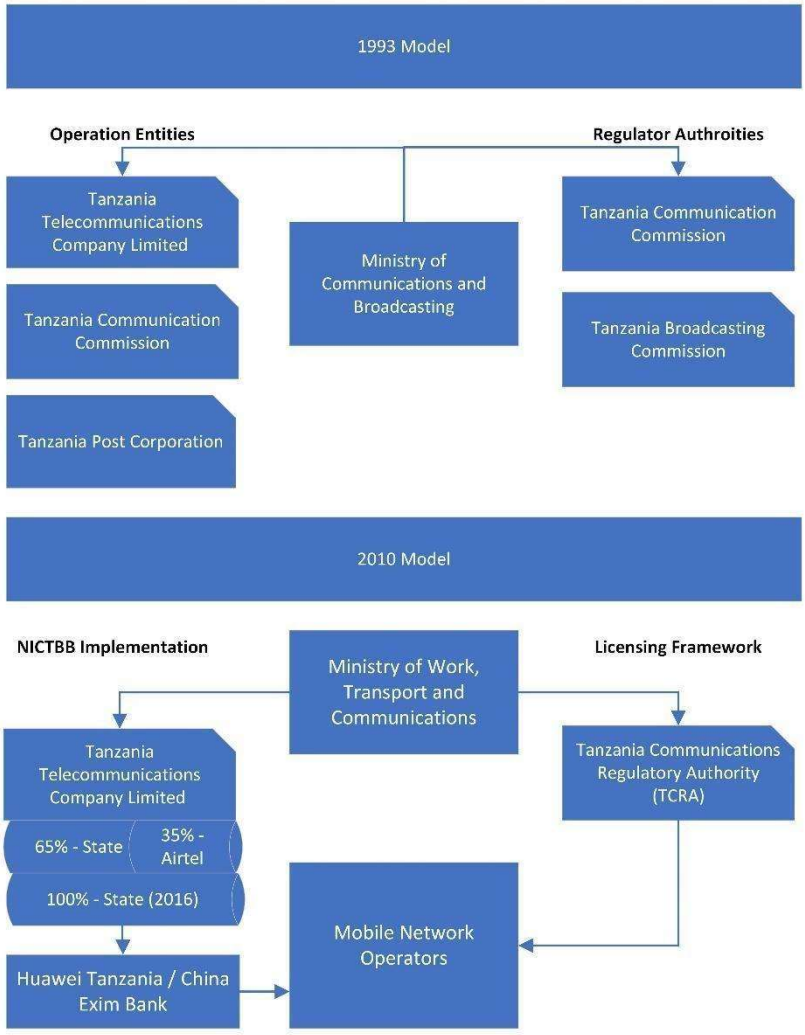
DataSource: NetworkReadinessIndex.org

The aspect that remains particularly problematic for the digital transformation of Tanzania is the level of absorptive capacity across local businesses. Tanzania is ranked lowest in the world in terms of the business spending on software engineering, and gross domestic expenditure on research and development by businesses (Network Readiness Index Report, 2020). On the one hand, this implies that ambitious plans of the government are not met with corresponding vision among the small- and medium- enterprises. It is estimated that only 1% of the medium-size enterprises in Tanzania consider investing in creating their own website in the near future. On the other side, such a considerable gap between the government and private sector is attributed to the industrial mix of Tanzania – with the most SMEs being concentrated in sectors which do not require high levels of automation, marketing, and research investments (gold mining, quarries, travel and tourism) – other East African countries are ranking higher on this indicator due to the larger share of SMEs being concentrated in such domains as Finance and Insurance, Logistics, Hardware production, among others.

1.3 Tanzanian Regulatory Framework in the ICT Sector

The discussion of the disconnect between the public and private sector within the Tanzanian environment necessitates to clearly outline different layers of the programme and policy-making in this domain. The first regulatory acts in Tanzania were adopted in 1993 – the Tanzanian Broadcasting Services Act and The Tanzanian Communications Act – and created the preconditions for market liberalization of the first Information and Communications technologies in the country. In 1994, the first ICT actor commenced its operations, *Tanzania Telecommunications Corporation Limited (TTCL)*. TTCL became the first telephony services provider, and it was fully state-owned until its partial privatization in 2001, the decision that was reverted by the authorities in 2016. Today, TTCL serves a dual role, both as a national communications solution owner and a mobile service provider (UNCTAD, 2020); but its primary function is administration of the *National ICT Broadband Backbone (NICTBB).*

The broadening scope of digital technologies and communications tools led to the demand for a more enabling legal framework, which led to the 1993 Acts being replaced by the Electronic Communications Act in 2010. The important change in legislation that ensued by this Act is the introduction of the Converged Licensing Framework that regulates acquisition, extension, and commissioning of licenses in the ICT domain, which are issued and overseen by the *Tanzania Communications Regulatory Authority (TCRA*). The Licenses framework encompasses the full cycle of IT development – from establishing facilities and equipment provision to online content publication, website registration and software applications' release (UNCTAD, 2020). On top of the Converged Licensing Framework, TCRA is solely responsible for the regulations in the telecommunications market, including price regulation, creating the rules and thresholds for market entry. Therefore, the model of interaction between operation and regulatory authorities went through the transformative path since 1993 with some of the entities losing the duality of regulatory and operational statuses (Graph 6).



Graph 6. Tanzanian ICT Regulatory and Operational Framework

The *Ministry of Work, Communications and Technology* is responsible for coordination of the strategic initiatives, policy formulation, and overall coordination of ICT development programmes (Esselaar & Adam, 2013). It also manages government bidding for infrastructure projects, identifies international cooperation priorities for the technological sphere in the country. NICTBB ("backbone") project which the Tanzanian government embarked upon in 2009, became the crucial development in the modern telecommunications history, the Ministry established the NICTBB as a separate operational division in collaboration with TTCL, with all the organizational activities of the latter being subsumed under the newly established entity. For the rollout and maintenance of the backbone, the NICTBB partnered with *Huawei Tanzania* and utilized funds provided by the credit line of the *China Exim Bank* (a total cost is estimated at 270

million USD) (UNCTAD, 2020). All mobile network operators and IT services providers are connected to the backbone and pay corresponding maintenance fees to TTCL.

In recent years, the regulator (TCRA) and Ministry of Work, Communications and Technology (MCT) issued a number of policy and strategic documents that predetermine the direction of technological path Tanzania is going towards. The most important of them are summarized in the table below. From the list, it can be inferred that the country's regulator TCRA is taking a rather interventionist approach to regulating the IT and, particularly, telecommunications market. The range of most recent laws were implemented to restore the full right of the regulator's interventions into tariffs, price formation as well as setting criteria for legality of operations; the authority that the entity partly lost due to liberalization laws it implemented in 2016.

Type	Date	Entity	Description
Digital Strategy Project	May 2021 (2021-2026)	MCT/The World Bank	150 mln USD ICT development aid project driven by IBRD; IBA and The World Bank, focused on ICT infrastructure improvement for businesses and increasing coverage in rural areas
	June 2020 2020-2025	MCT/President of Tanzania/UNDP	Tanzania Development Vision 2025 – identifies the strategic shift towards building capacity as the most important challenge of ICT development for the next 5 years
Regulatory	April 2021	TCRA	Online media content licensing re-launch. Previously online media content licenses were suspended due to the corresponding President's directive
	March 2021	TCRA	Data bundles implementation
	January 2020	TCRA	Electronic and Postal Communications Law. The law prohibits information and communications technology providers to liaise with foreign vendors without pre-approval from TCRA
	January 2020	TCRA	Electronic and Communications Tariffs Law, 2020 – identifies that tariffs should be based on incremental long-term costs and broadens the scope of possible intervention from the TCRA in case of market failure.

Table 2. Summary of latest regulatory and strategic developments in Tanzanian ICT

Strategic Projects – Digital Strategy Project and Tanzania Development Vision (TDV, 2025) have two underlying themes in common. First, they identify the transition towards training professionals as a crucial milestone to continue economic growth in the country. Digital Strategy Project prescribes 35% of its budget to capacity development, whereas the Tanzania Development Vision 2025 stipulates that "appropriate skills and capabilities would have to be put in place to meet the new opportunities presented by ICT development. This task demands that adequate investments are made to improve the quality of science-based education and to create a knowledge society generally". Second, "Good governance" pillar is attributed particular emphasis in both strategies. The strategic documents set out digitalization of government services as the means of achieving citizen engagement into the digital transformation. It is expected that once Tanzania reaches 70% internet penetration rate (which is planned to achieve by the end of 2023 in line with the Digital Tanzania Project), most of the ICT development aid will be reallocated towards the e-government projects.

It is evident that the public sector innovation remains the top priority of the Tanzanian government and international aid organizations. The lack of focus on these areas would reduce the international development aid as those are the areas crucial for addressing corruption, mismanagement, and kleptocracy. Nevertheless, some of the problematic areas remaining out of the equation, and has to be addressed within the near future to sustain ICT-enabled economic growth;

- I**mplementation of the regulatory framework for e-Commerce activities.** With a full-fledged introduction of alternative and digital payment systems, and proliferation of the international players to the online delivery services, the lack of the rigid regulatory framework leads to the lack of trust in this viable domain of ICT growth.
- While investments in capacity development and training are underlined in the policy documents, there is a lack of focus on **digital entrepreneurship to address the gap between the government and business dynamics of innovation.**
- **Awareness building activities should be given a higher priority.** While the fact that most of the services that became available to Tanzanians with the internet penetration has not translated into higher connectivity due to high smartphone costs, the lack of awareness

posits another important problem. Recent surveys show that 80% of the population were not aware of the online payment services that were implemented by the government in 2019-2020 (Parks et al., 2021).

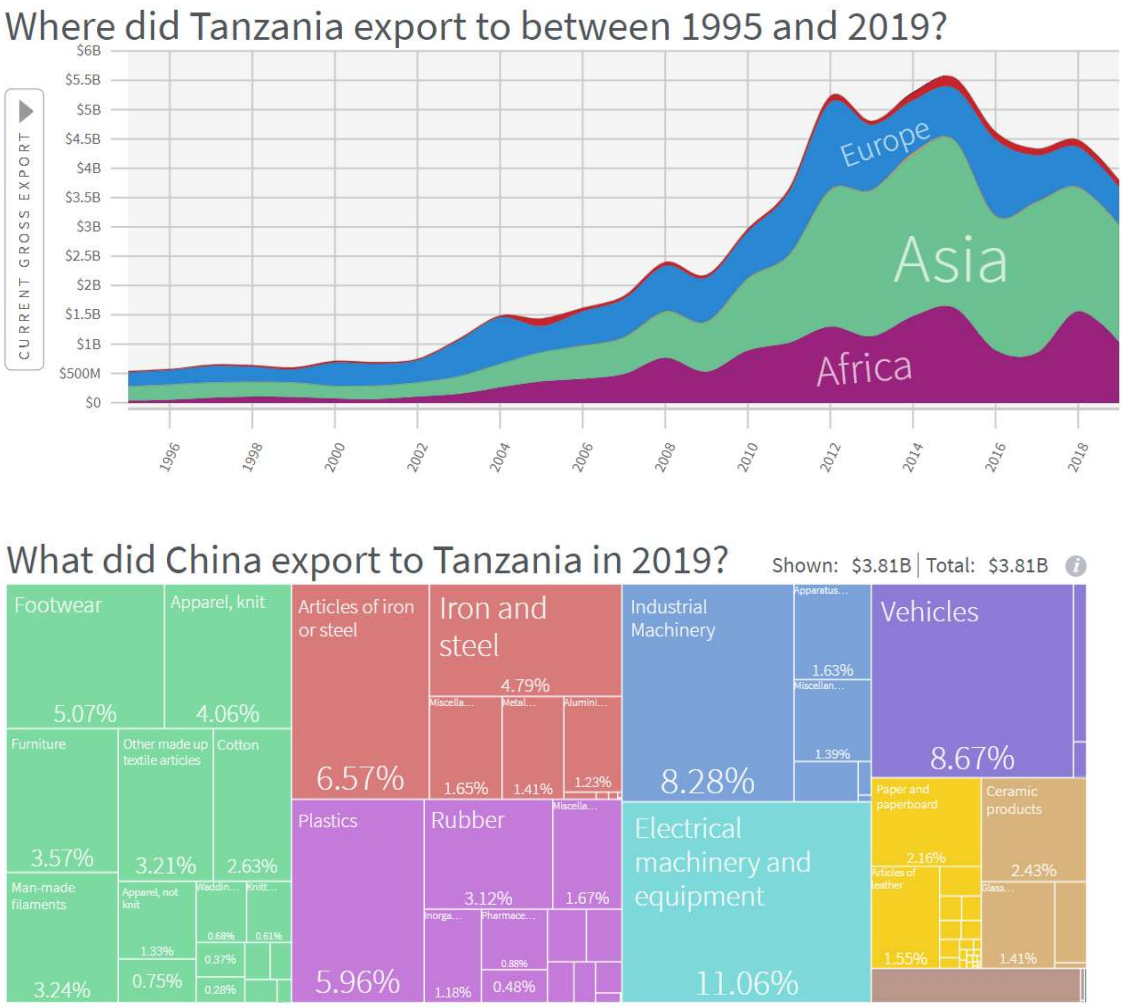
- **High fragmentation of the ICT domain**. There is a need to empower "open innovation" and knowledge sharing among companies to overcome fragmentation of the market (Ortiz-Crespo et a., 2020).

1.4 Sino-Tanzanian Cooperation in ICT and Beyond

As we explored in the above sections, Chinese big tech provider Huawei and the state-owned China Exim Bank were involved in implementation of NICTBB, Tanzania's core infrastructural project and the most important ICT development. In order to provide further context for the current research, there is a need to examine more closely the full spectrum and evolution of the Sino-Tanzanian cooperation.

China is the largest trade partner of Tanzania, with the trade between countries accounting for 21% of the cumulative trade balance of Tanzania; China is the third largest export destination following India and UAE (7.78%) and Tanzania's largest source of import (29%).

The role of Asia-East Africa connectivity on the economic growth of the latter in the 2010s is gaining worldwide attention, however, the history of close cooperation between China and Tanzania has a longer timeline. TAZARA Project, the railway line connecting Dar Es Salaam in Tanzania and Kampiri-Mposhi in Zambia, which was constructed in 1976, holds up a foundational legacy for Chinese presence on the African continent. While TAZARA Railway has passed its peak traffic and socioeconomic significance, it has become a symbol of Chinese commitment to the infrastructure upgrade of African countries as the major pivot of bilateral cooperation (Monson, 2013).



Graph 7. Tanzania's export portfolio (Hausmann 2020)

Intensification of the trade across the Indian Ocean is the predominant explanation for the expansion of Asian portfolio in the Tanzanian trade balance. Port of Dar Es Salaam represents a key gateway not only for Tanzania but also for the adjacent landlocked countries, accounting for 90% of the trade operations of the country. The port infrastructure alone contributes 6.4% of the country's GDP (Dar Es Salaam Municipal Council, 2019). Therefore, expansion, renovation and maintenance of the Port of Dar Es Salaam (owned by the government of Tanzania) has been the question not only of economic development strategy but of national security. The port has undergone several stages of upgrade, with Chinese investment holdings providing the services. For instance, in 2017, when the accommodating capacity of the port was doubled from 35000 tonnes to 70000 tonnes, the government contracted Chinese Harbour Engineering Company (Hönke, 2018; van Giezen et al, 2021). Following the success of the project, Chinese and

Tanzanian governments have been leading negotiations regarding the ambitious 10-billion project of constructing a new port that is set to become the new export hub of East Africa, Bagamoyo Port (Alden et al, 2021). The agreement was reached between Chinese Merchants Holdings, Oman Reserve Port Holding and Tanzanian Government in April 2021 on launching the construction, which will become the largest infrastructure project in Tanzanian history (van Giezen et al, 2021).

The boost in trade between Tanzania and Asian countries, as shown in the chart above, is propelled by the ambitions of Indian and Chinese governments over the Indian Ocean regional trade control. The Indian Ocean is accommodating 75% of the world's oil transit, prompting India and China to strive after taking the leadership role in the trade dynamics, regional integration, and infrastructure investments (White, 2020). Developments of the ports in East Africa, including Bagamoyo Port Project, Dar Es Salaam Port renovation, and Mumbasa Port Expansion (Kenya) and the high-speed railway connection between these ports are outlined as a part of the *Maritime Silk Road Initiative, one of the two pillars of the "One Belt, One Road'' Initiative.* Chinese government repeatedly underlined that the commitment of East African countries to "One Belt, One Road" initiative is aligned to the strategic goals of African development considering that they will address the "key underlying issue behind the underdevelopment of these economies, which is the lack of modern infrastructure" (Forje, 2018). Mukwaya & Mold (2018) modeled the impact of the "One Belt, One Road" initiative on East Africa, and identified that per modest estimations the project will boost country's export by average of 190 mln USD annually and increase welfare by ca. 1 bln USD.

The study by Blanchard and Flint (2017) has established that the Maritime Silk Road Initiative is not only "about hard infrastructure, but the development of soft infrastructure is an integral part of the story too". Soft infrastructure herein refers to the combination of the bilateral trade agreements liberalizing markets and tariff formation to benefit China, capacity-building, business model and ideology import (Blanchard and Flint, 2017). Blanchard (2020) further argues that there persists a variation between how the Maritime Silk Road project is perceived in Tanzania and other African countries, with Tanzania being the stronghold of skepticism towards Chinese-led development projects. Comparing success of the initiatives under the aegis of Maritime Silk

Road in Ethiopia and Tanzania, the author argues that the fact that the former has already developed numerous projects with a total value of several billions USD, whereas the latter has taken 5 years to negotiate the hallmark project of Bagamoyo, “has nothing to do with dissimilar development priorities or involvement of India” (Blanchard, 2020). The very slow process of Tanzania’s integration into the Chinese Initiative only stems from the geopolitical concerns and additional scrutiny the Tanzanian government allocates to projects that are led under Chinese leadership.

In line with this, Makundi et al. (2017) underline that the commonly held perception that Tanzanian government has a more lenient and “weak” diplomatic stance in regards with Chinese soft diplomacy is erroneous (Hanusch, 2012). While Tanzania was among the first African countries to recognize Chinese government as a result for a decade-long “infrastructure for diplomacy” strategy employed by the Chinese in the 1960s, following the success of this tactic, recognition of Chinese government and completion of TAZARA, the cooperation has been interwoven with a range of security and diplomatic issues (Makundi et al., 2017). This tendency is reflected in few strategies – delayed projects (such as Bagamoyo Port Project, approval of which took 7 years) and tight control measures, softened loan conditions to avoid debt crisis. The Tanzanian public sector debt has increased twofold in the post-Crisis period (2008-2018) (Stein, 2019).

There is a limited research discussion on the latest developments in Sino-Tanzanian relations, however, drawing upon the media discourse and public sector strategies, certain trends that govern the near future of these relations can be identified (Shi, 2019). First, state actors in these relationships are behind pushed to the background by the private actors. Big tech companies with presence in Tanzania – Huawei and CITCC are the major interest groups defining the future development. This is even documented in the strategy of “Chinese Engagement” presented by the Tanzanian Ministry of Foreign Affairs in 2017 at Forum for Africa-China Cooperation (Shi, 2019). Currently, Chinese investors are hardly experiencing pressure to engage with any local actors in Tanzania beyond the Tanzanian government. This is limiting the knowledge transfer and sustainability of the projects delivered. In line with discussion above, this is reflective not only of the Chinese commercial sector engagement in Africa, but the lack of private sector engagement

and preconditions for knowledge transfer across the private actors is the structural problem of Tanzanian economy. Second important trend is the overall diversification of the Chinese engagement across Africa with a strong footprint of Chinese commercial sector, ICT infrastructure, military engagement in Sudan, Ethiopia, Kenya, Uganda, among others (Shi, 2019). In this context, despite being the most politically stable country in East Africa, the defensive and tightening position of Tanzanian public sector has led to reallocation of Chinese resources to other African countries. The new strategic framework adopted in 2017 is seeking to turn this trend around by positioning the country as the most important economic hub of the region.

2. Theoretical Framework

2.1 ICT Development, Cybersecurity and Transparency

Information and communication technologies are widely considered as tools for achieving productivity growth, *providing developing countries with a sustainable path for growth and sustaining political power, and increased transparency in governance.* In line with Arsene (2013), the relationship between ICT development and political institutions is twofold. On the one side, it provides political institutions with the toolbox for enhancing transparency, reinforcing the democratization process; empowering civil society, and increasing efficiency of local governance. Due to the fact that the ICT development and digital transformation of non-ICT sectors are related to bearing political commitments and ambitions of democratization of the country, the *question of foreign direct investments into ICT projects becomes sensitive* (Zhang et al. 2016). While the governments are being provided with an adequate infrastructure to realize their political commitments, they incur considerable risks to their national security through providing access to sensitive data and data management systems (e.g. election interference).

On the other side, ICT-intensive growth transforms the way the development projects are being carried out, and in light of that most of the international developmental organizations had to rethink the way the projects are being implemented (Arsene, 2013). Development projects that either international non-governmental actors implement or that are obliged to be implemented by the local governments with funding and support of the international community have to involve the rollout of ICT infrastructure. For instance, programmes targeting food security – heavily rely on ICT infrastructure for smart disbursement (WFP), programmes aimed at gender equality rely on knowledge and data management systems (e.g. USAID projects in Africa). This implies that economic development and aid projects become entangled with large-scale international ICT sector. And in the context of African countries, where ICT infrastructure and capacity are still emerging, this implies heavy reliance on *new and foreign vendors* – which became an opportunity for relatively affordable and quick to roll out services of the Chinese tech sector to capitalize on.

Therefore, it comes without surprise that a relative liberalization of ICT markets across Africa coincided with a strong proliferation of Chinese big tech companies since the beginning of 2000s.

Opening of the government bidding to foreign investors led to the situation where Huawei and ZTE were able to use their price advantage to develop a strong footprint. A study by Atlantic Council identified that Huawei, the controversial Chinese telecom giant, was responsible for 50 per cent of the 3G network rollout, and more than two thirds (71%) of the 4G network rollout in Africa (Zaamout et al., 2019)

Network coverage is an important part of the government's security and strategic development. First, higher internet penetration is a prerequisite factor of economic growth. Higher connectivity ensures increase in productivity of economic resources. Access to broadband services leads to economic modernization and allows more productive utilization of businesses' capital and labor resources. According to the World Development Report (The World Bank, 2016), internet access alone contributes to 3.4 percent of the global GDP, where its contribution to the annual growth rates ranges from 15 to 24 per cent across different groups of countries. With each year, the importance of internet proliferation is growing as the further global production and services modernize, the greater the importance of the businesses' ability to innovate (The World Bank, 2016). Second, the network rollout is positively correlated with countries' bilateral trade (Xing, 2018). The higher connectivity, the more firms have access to regional and global markets, and the higher ability to reach new markets as well as exchange knowledge, innovations, and other resources with a more established market.

Considering these factors, handing over the development of the telecommunications infrastructure to the Chinese big tech companies has raised the concerns among the Western media and international actors. It provides Chinese companies with a leverage over the economic growth, dictates job creation providing Huawei and ZTE with a leverage over successes of the governments' economic policies and therefore sustainability of the current government regimes. This mechanism is widely discussed in the strain of research that is focused on China's soft power across the developing countries (Mano, 2016; Gatere, 2019).

What exacerbates the latitude of China's exercise of *soft power through telecom infrastructure rollout is the business model those projects are hinged upon*. Over the last decade, the mode of cooperation between state and non-state actors to rollout telecom networks started to shift from on-project basis to long-term cooperation projects. Thus, African governments committed to the

long-term projects of infrastructure modernization such as the Digital Silk Road, the project joined by 16 African countries, which pervades all aspects of ICT infrastructure, from smartphone distribution and network deployments to e-commerce and online banking (Sen & Bingqin, 2019). Funding of the portfolio of these projects, which is estimated to reach 9 billion USD, is guaranteed by state-owned Chinese banks (Ministry of Foreign Affairs of China, 2021). Whereas African governments would not be able to implement such large-scale projects of economic modernization without access to low-interest Chinese funding, this also means that the future development path of these countries is controlled by Chinese soft power. Therefore, while one can ask: "If the telecommunications equipment is so vital for economic growth of the country, whether it is reasonable for African countries to rely so heavily on foreign investment?" The answer is that there is a lack of alternatives.

The soft power triangle between China, African governments, and Huawei/ZTE has another aspect of linkage and cooperation which lies in the space of *cybersecurity*. On the one side, African governments are provided with a Chinese model of data sharing, which enables them to use the technology to control the civil society and population of the countries at large. The prime example is the Ethiopian regulatory framework which was adopted in the similar approach to the Chinese ICT sector, with the Ministry of Communication shaving a total control over licensing of telecom equipment and data governance across the private sectors, which underlines the fact that the provision of the infrastructure projects may be accompanied by the shared legal and political practices (Polyakova & Meserole, 2019).

There are numerous reports of the usage of such technologies as face recognition, or extracting internet traffic information from Chinese providers to address unrests and silence opposition forces (e.g. in Uganda and Ethiopia) (Noesselt, 2019). On the other side, China is provided with an opportunity to have access to African public data for bolstering its geopolitical agenda. The Chinese regulatory framework is characterized by stringency in obligation of all corporate-sector actors to share data with the Chinese government. Chinese government may potentially make use of its data in the number of ways;

- Controlling media and civil society narratives by using public data or private data shared by government officials

- Providing governments with the tools on which they would rely for their own political agenda and sustaining in power (toolbox for curtailing unrests, implementing democratic processes)
- Promotion of the positive view of China and countering anti-Chinese propaganda
- Direct data intrusion (e.g. elections manipulation; intelligence data gathering in strategic sectors such as healthcare and military)
- Suppression of potential competitive forces in other non-ICT markets in Africa.

Most importantly, provision of the telecom infrastructure and broadband equipment opens up for Huawei and ZTE opportunities to take over adjacent domains of ICT and win contracts on provision of other business services. *One of such services that is critical for cybersecurity is the rollout of data centers,* specialized centers for integration of private and public data to accommodate the growing data generation. Once the 3G/4G/5G networks are rolled out, governments are seeking the opportunity to expand its data center infrastructure and building upon the previous collaboration with Huawei and ZTE, as well as accessing low-interest funding from the long-term collaboration initiatives – Digital Silk Road and Smart City – those companies are the first-option providers in most of the cases (Zaamout et al., 2019). Over the last years, a number of large African countries, including Tanzania, Cameroon, and Kenya invested more than 200 mln USD into the setup of government data centers in cooperation with Huawei – in all cases the projects were financed by China Exim Bank (Tang, 2021).

The setup of data centers gives the opportunity for *direct and indirect data exfiltration*. Direct data exfiltration is performed through data theft through the established infrastructure as in the case of the African Union headquarters leak was reported to transmit data from the AU every night for the period between 2013 and 2018 (Carrozza, 2018). The leak took place due to centralization of all data infrastructure using Huawei FusionCloud Desktop Solution and the fact that applications and data security protocols were outdated (Shoebridge, 2018). Indirectly, data exfiltration can be performed through intentional selection of the infrastructure objects that might be susceptible to data sensitivities. For instance, Chinese providers might intentionally use outdated technologies and inefficient algorithms for encrypting communications (Shoebridge, 2018).

Last but not least, the intersection between ICT development and democratic governance is manifested through capacity-building endeavors. Multi-million investments into the infrastructure rollout are accompanied by the efforts to promote IT and technological competence across the board. This means that the knowledge and skills of the workforce in the recipient countries are being determined by Chinese big tech companies (Tang, 2021). In Tanzania, Huawei launched training programmes for more than 1500 professionals, which accounts for 32% of the high-skilled technology-related workforce in the country (Huawei Annual Report, 2020). In neighboring countries, Including Kenya and the Democratic Republic of Congo, Huawei and ZTE partnered on the establishment of training centers to prepare telecommunications experts (Tang, 2021). The related government security risks are evident through potential ideological indoctrination, and training of the personnel in accordance with the Chinese business model based on disregard towards intellectual property rights, high centralization of the resources, and lack of transparency. While it is still debated in research and tech communities whether this trend has ideological or geopolitical pretexts, it is undeniable that the fact that China is almost solely responsible for providing training to the ICT experts in the recipient countries will have far-reaching consequences to the country's security and governance.

2.2 Securitization Theory in ICT Context

In this section, we will employ securitization and desecuritization theories of international relationships to extend the discussion of the Sino-Tanzanian relationships and the underlying national security concerns to further re-embed these two themes in the Analysis section.

Securitization has been among the most popular analytical frameworks to theorize geopolitical aspects of international relations. In the most general terms, securitization theory involves the process of transforming a non-political or soft political agenda into the issue of national security (Nyman, 2013). Buzan et al. (1998) defines *securitization as an inter-subjective establishment of the existential threat providing it with saliency to initiate long-reaching political implications.* The framework presumes that no political or economic issue is an objectively security issue per se,

but the securitizing actor transforms it into such. The emergence of the securitization and the success of the political implications generated by it are predicated upon the ability of the security issue to generate commeasure emergentist or sensitized reception among the public audience (Buzan et al., 1998). Securitizing actor, be it a political leader or any other representative of power, uses rhetorical instruments to achieve this reception and create the perception of emergentism, existentiality of the threat (Nyman, 2013).

Therefore, the general logic of the securitization theory contains the following components, the presence of which has to be discerned in the given context in order to apply this framework;

1. **Existential Threat –** the political (non-military) or economic issue that is magnified or socially constructed into the issue of security.

2. **Securitizing Actor** – the political leadership that is interested in pursuing the given political, geo-strategic or economic agenda in response to the existential threat.

3. **Audience** – as, in accordance with the emphasis of Buzan et al. (2018), securitizing is "inter-subjective and socially constructed", the referent audience plays even a more important role in "securitizing" than Securitizing Actor.

4. **Rhetorical Devices** – political appeal towards the referent stakeholders that can be affected by the securitized matter; citizenry, international community, or other stakeholders.

5. **Emergency Action** – plan of mitigating issues that are proposed by the securitizing actor to alleviate or prevent the consequences of the existential threat.

The most popular case interpreting the securitization theory is the War on Terror in the response to 9/11 terror attack, which spurred interest in this theoretical framework; however, most of the studies in this domain remain largely Western-centric (Ezeukafor & Kaunert, 2018). Attempting to re-conceptualize the securitization theory in the African context, Ezeukafor & Kaunert (2018), identified that the difference between Trans-Atlantic and African model of securitization, is that the securitizing actor is mostly seeking *reception among the narrow circle of elites* (including elites of neighboring countries, regional organizations and NGOs) rather than a general public. This implies different methods that are used to securitize the issue, for instance, the role of online communication channels or media control is diminished in contrast to the Western-Centric framework.

Can ICT infrastructural developments and the ICT sector at large be the matters that are securitized? The growing bulk of research has attempted to reintegrate this framework using the issues of cyber security in particular (Lacy & Prince, 2018; Hansen & Nissenbaumn, 2009). The recent attempts to securitize cyber threats in the form of potential election meddling have been made reciprocally by the West and Russian Federation. Such cyber threats have been at the forefront of media discussions in both geopolitical rivals, which reinforces the presence of rhetorical arguments and importance of media channels for existentialization of the threat (Kasper, 2014; Lacy & Prince, 2018).

In parallel with omni-presence of the digital infrastructure across the public sector, the ability of the cyber-security related concerns to be transformed into security issues has considerably grown over the last years (Lacy & Prince, 2018). Just a decade ago, they were more or less contained to the organization-level with most of the cyber-security infringements would not be described as “catastrophic” or as an “existential threat” such as manipulation of tender bidding or personal information leakages. Taking in mind that it is the “audience” rather than “securitizing actor” that determines the ability of the issue to securitize, there was a limited latitude for these matters to be politically magnified. Today, however, both the complexity of data infringements and digitalization of the key strategic industries has grown drastically.

Moreover, political processes in developing countries and digital technologies became much more interwoven. Digitalization brought diversification into the way political elites may interact with digital technologies to influence the broader political and geopolitical agenda. These include the above-mentioned election interventions – which predetermine the way political process would be driven to in the given country for the coming years, might establish the political rule loyal to the geopolitical stakeholder, and provide a soft power alternative to the military interventions and staged coup d’état (Buchanan, 2016). This led to the fact that the technological multinational corporations (“Big Tech”) became independent geopolitical entities. Political elites found themselves dependent on the technology providers in regulating many aspects of political life, which might be manipulated to form the political agenda in the country. Software can be used to spy on political opponents, data feeds political investigations, monitoring systems providing leverages of social control etc. (Cavelty, 2020).

2.3 Desecuritization of Cyber-Space

Despite their growing severity and penetration into different areas of socioeconomic life, it is evident that cyber-security threats are less intransigent in the securitization framework than other issues. Natural disasters, risks of military conflict, and global problems (climate change, pandemics) pose a more tangible risk to societies and are absorbed easier as security threats since the consequences of them over the lives of the "audiences" may be irreversible. Desecuritization is another component of the Securitization Framework applied in this study, and as defined by Buzan and Wæver (2003, pp.486), *Desecuritization* refers to a *process of downgrading or ceasing to consider some non-political agenda issue as an existential threat and withdrawal of the emergency actions that were supposed to be entailed by this threat*. In the most general terms, in contrast to securitization process that frames a non-political issue into an existential threat, desecuritization takes exactly the opposite steps to alleviate tensions and to manage the threat rather than to extend them into emergentist policies and regulations (Burton & Lain, 2020, p. 462).

Buzan and Wæver (2003) and Wæver (2015) identified the number of the core paths for desecuritization policies that are applied generally to different contexts. First is to *disconnect the issue from the security context altogether* (Buzan and Wæver, 2003). This means that even if the initial rhetoric discourse that was propelling the severity of the matter may continue, it should be totally detached from the security issues such as national security and threats to the well-being of the population. Second is to *avoid social and inter-state security dilemmas (Burton* & Lain, 2020). If the issue was already securitized to a considerable extent, building trust and cooperation between adversaries is the method of retracting the previously followed path of emergentist plan of action. Third path for desecuritization *is re-embedding the securitized issue into quotidian domestic politics* – that is outlining achievable objectives and bringing the consensus around on how those objectives can be controlled within the legal and political life of the country. Instead of promoting concerns over the Existential Threat, the de-securitizing actors replace it with the understanding of "inevitable" measures to be taken to address some parts of the threat that can be controlled by the society.

Path for desecuritization	Copenhagen School Explanation (Burton & Lain, 2020; Wæver (2015)	Cyber-Security Context
Disconnecting the Securitized Issue from the security context	-Retaining the Securitized Issue on political and media agenda -Re-branding the issue taking out any components of national security, economic development, well-being	-Changing the tone surrounding cyber-attacks changing the narrative to more constructive -Narrowing done the discourse around cyber-security to significant and insignificant threats, and focus the media discourse on the latter
Overcoming social and inter-state security dilemmas	-Building trust and cooperation between adversaries -Showcasing multilateral cooperation as the way of threat prevention	-Multilateral agreements to control cyber-security -Replacing the "otherness" of cyberattacks and turning the rhetoric away from cyber-attack instances towards "cyber security as a common threat"
Re-embedding Securitized Issue into quotidian domestic politics	-Fragmentation of the initial threat into the number of separate issues that can be controlled or effectively addresses within the domestic political agenda	-Recognition of cyber-security as a global challenge and shifting responsibility away from the state apparatus towards Big Tech, multinational actors -Compartmentalizing different aspects of cyber security and addressing them through well-defined objectives and frameworks within legislative and sociopolitical agenda

Table 3. Summary of the paths for desecuritization discussed in the literature.

What makes the choice of the path for desecuritization challenging is the lack of clarity of who has to become a *desecuritization actor* (Sanahuja, 2021). The bulk of research within the Copenhagen School predominantly refers to the cases where the de-securitizing actor is the same

as securitizing actor – the government, military, and public sector officials responsible for securitization. However, in the context of cyber-security, the undertaking of desecuritization of cyber threats would be complemented by the number of long-term interferences with political interests of the securitizing actor. If the government takes a leading role in downplaying and toning down the cyber security issues, it will undermine different avenues of bureaucratic and political pressure in the future (Burton & Christou, 2021). Following, desecuritization, securitizing actor still would need to be able to exert influence from the strengthened cyber defense and justification of changes in legislation surrounding data and ICT regulation – as in many developing countries, those are still at rudimentary stages, the governments prepare for implementation of, in many cases, unpopular measures to control data security (Barnard-Wills & Ashenden, 2012).

In line with Burton & Lain (2020), *desecuritization* can be led by the societal approach that combines the awareness raising and capacity development. Any type of technology has a property of *shared ownership*, that is, it can be transferred, shared through effective knowledge management strategies. Decentralizing knowledge sharing and transferring technological know-how in this framework can be considered as a potential path for desecuritization. With larger number of private stakeholders, both business and individuals, establishing ownership over technology directly (etc. access to government data, public databanks) or are equipped with the toolbox to manipulate technology (through enhanced technological awareness and skill set, cyber-security competence), the referent Audience will mitigate the Cyber-Security threat autonomously. This notion has been gaining consensus in the policy-making domain over the past few years, with the policy shift towards the requirements *to "open innovation", and transfer knowledge from Big Tech to local actors*. *The Tanzania Development Vision 2025* is a case policy-document that corroborates this tendency. At the backdrop of the growing concerns over dependency to China on data and ICT infrastructure, Tanzania, and the range of other African countries are exploring opportunities to oblige and promote transfer and knowledge technology from Chinese tech giants to local actors This strategy does not hinder the government from the future tightening of regulations tackling cyber-security and data ownership, but at the same time provides the concerned stakeholders with a sense of control over the securitized issue.

3. Research Design & Methodology

3.1 Rationale for Research Design

The use of an inductive, qualitative approach is interdependent and pre-determined by a spectrum of observations, interactions, unforeseen experiences that formed an hypothesis that is catalyst for the constructivist ontological perspective ascribed in this exploratory study. Given the position that *''history is not some kind of unfolding or evolving process that is external to human affairs''* (Jackson & Sørensen, 2010 p.211). Hence, observing China's emergence as a global geopolitical power over the past two decades growing in cohort with the disruptive power of ICT networks (Xing, 2018). Noting these developments and applying a constructivist view with regards to China's prevailing expansion into the African ICT market, as well as the security issues arising from increased connectivity, networks and lack of digital literacy to govern cyberspace inspired the problem formulation. Which in turn informed our qualitative interpretivist epistemological approach taken and the theoretical framework that guides our mode of untethering correlations and points of departure (Bryman, 2015).

Securitization framework components identified in the theoretical framework of the current study are best addressed through the principal theory of constructivism, denoting with it a epistemological interpretivist mode of analysis, as we attempt to decipher the reality observed and constructed by us (Hunt & Colander, 2017). Qualitative interpretivist approach, intersects with both a constructivist view of the world as well as (**de)securitization,** as the use of narrative and framing of issues are a means of addressing national security. Since, this paper seeks to deepen discourse on preemptive desecuritization of the ICT sector being an integral aspect of functional cooperation between China and Africa by using Tanzania as a case study, an inductive interpretive exploration is befitting.

3.2 Ontology & Epistemology

Ontology

In order to accurately assess the validity of the findings in this study, we need not share a similar ontological framework, merely be willing to complement the validity of the findings. Since the problem can be approached from various ontological perspectives, constructivism is chosen as it in the context of exploring cooperation patterns, it provides the most optimal avenue to interpret the finding, by not limiting the pursuit of functional cooperation to for example a realist lens of international relations and its power driven values, centered around the sustaining of the state (Jackson & Sørensen, 2010). Hence, constructivism is applicable to this study as its main tenets propose that the world is as it is today due to an array of interactions between, systems, actors, structures, and social interactions that denote the current state of affairs, and what will be (Wendt, 1992). Given our objective to understand how a functional relationship in the ICT sector can be formed through desecuritization, constructivism was a given ontological worldview to apply.

Considering the analysis examines the interplay of various variables that have structured China's ICT relations with Tanzania, the constructivist approach which accounts for the tools people employ to comprehend the world around them, are a byproduct of interactions that are fluid and changing ever so more rapidly, due disruptive technologies, and since this perspective values the use language in the shaping of the world, it was a seamless choice (Wendt, 1992). In summary, our constructive lens has informed our epistemological choice, how we uncover or explore the hypothesis, which is by way of an interpretive narrative analysis (Esser & Vliegenthart, 2017).

Epistemology

Epistemology is how we pursue truths in the reality we inhabit, as such it is both informed by the ontological point of departure, hypothesis and inductive process (Hunt & Colander, 2017). As such this study approaches the analysis in an interpretivist manner, employing narrative analysis to distill themes and sentiments analysis to uncover the avenues to as close to utopian functionality between China and Tanzania as it pertains to ICT.

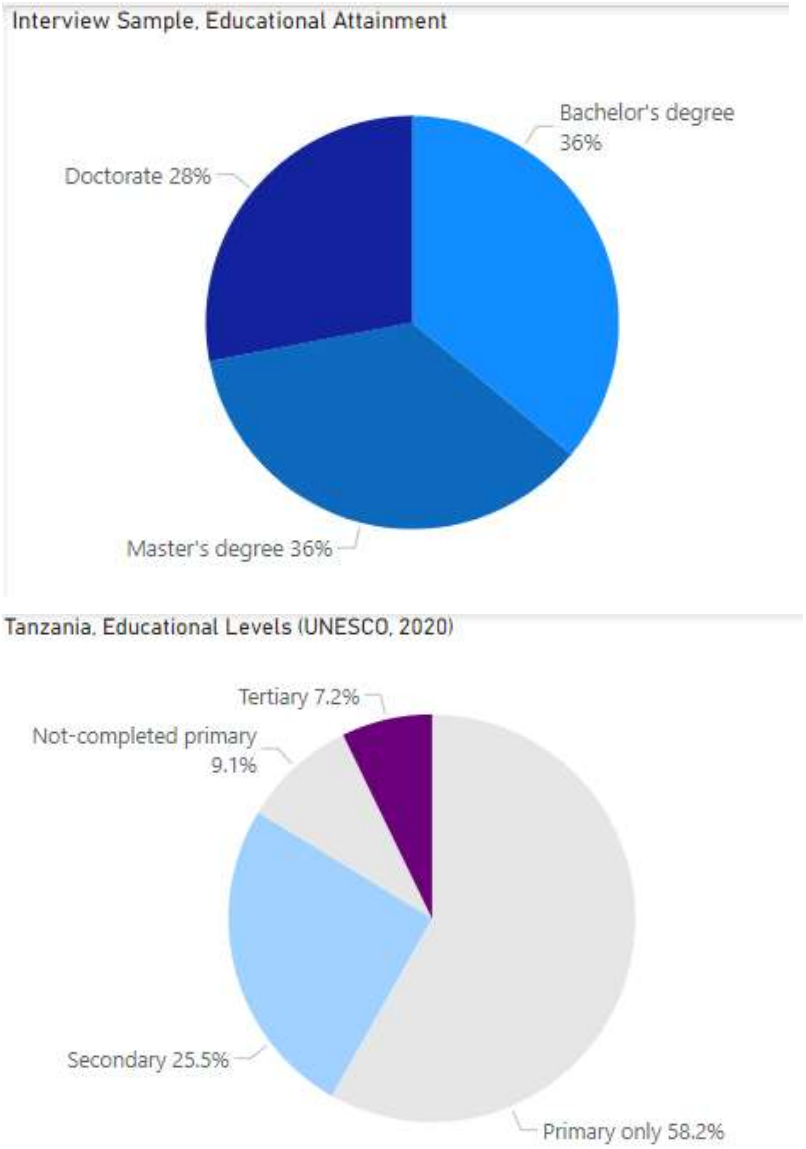
Interpretivism is a phenomenologist means to inference, that a person's view of reality shapes their reality, hence it is constructed both via externalization and internalization, hence it is complements a constructivist ontological approach, and bequeaths a structure for interpretation of narratives, legislature, discourse, and articles (Bryman, 2015). This interpretive approach to exploring, as Bryman further explains how states and individuals respectively are groomed in varying environments and contexts, thus a non-rigid interpretative approach lets researchers account for the multitude of variables entangled. In this project the interpretive approach is an avenue to understand states' individual context in order to frame and compare similarities and differences, in pursuit of comprehension of what is needed and what ought to be extracted for the functional framework to emerge.

3.3 Interview Methodology and Sample

Interviews were conducted over a span of two months between October and December 2021 via Zoom in an open-ended format. A semi-structured form with open-ended questions such as *How do you perceive China, Tanzania cooperation within ICT?* was applied due to a desire to elicit long responses in order to capture the full scope of the audience's sentiments (Jamshed, 2014). Within this form of interviews, the role of the researcher is merely to serve as conversational guide in an attempt to limit researcher bias creeping to audience responses, as such interviews were given time to ponder over questions as well as prodded ahead when needed (Jamshed, 2014). The interviews were structured from general to specific to avoid internalizing bias in responses by initiating the respondents' exploration process based on the content of the previous questions. In line with our interpretive phenomenology in an attempt to uncover perspective from stakeholders, purposive sampling was used to determine the demographic of interviewees (Emmel, 2013).

Meaning again going from broad to specific, to attain a representative sample of country demographics, as well as, purposefully selecting students, and business owners as theoretical high-end users of the ICT infrastructure in Tanzania. Among the **25 interview respondents, gender distribution is as follows; 4 (16%) – female, 21 (84%) – male respondents.** Mean age of the interview sample is 34 years old. Additionally, half the subjects were students with only one woman being amongst business owners. Our sample whilst seeking to be expansive, was within

our sphere of influence, meaning we sought out people within the travel industry, United Nation employees, through mutual contacts, as such **Tanzania expats make up 28 percent of respondents.** Furthermore, all interviews hold a degree beyond high school, this is not representative of the general education level in Tanzania, and as such presents a narrow elite with access, however it can be argued that those with access and opportunity will be the forebears of ICT innovation in Tanzania (Graph 8).



Graph 8. *Educational Attainment of the Interview Sample and Tanzanian Population in General Data Source: UNESCO (2021)*

The given subjects, whilst not representative of a proper sample of Tanzania, were within our means of access, and represent those elites with access to education and digital technologies. The semi-structured interviews, started with garnering basic background information of the subjects, and then ensued to pose open ended questions that went from a broad contextual question to upon response delving further into the subjects' narrative with follow up how and why question, that let the speaker keep talking (Jamshed, 2014). The objective being to create an environment and format questions that permit subjects to speak freely, as to uncover intended and unintended themes and sentiment within conversations. Upon finishing responses were transcribed in order to perform thematic sentiment analysis.

3.4 Qualitative Narrative Analysis

Narrative Analysis

Having provided a contextual overview of China and its ICT development projects with Sub-Saharan states, narrative analysis is applied to garner an insight into Tanzania's perspectives as well as discern how soft power is used, communicated and to what end. Soft power often denotes a negative meaning, however it can also be a tool of diplomacy and capacity-building strategies (Nye, 2012). Having conducted open-ended interviews with Tanzanian representatives ranging from business owners, NGO's, narrative analysis is a tool used to categorize themes, concerns contextualized within (de)securitization theory (Della & Keating, 2008). The limited sample of interviews narratives are a means of garnering stakeholders sentiments and themes relevant to ICT development to then compare to institutional practices, policies, and diplomatic efforts addressing security issues with other East African countries (Flick, 2014). Upon the analysis the narratives attained are discursively explored within the thematic categories of cyber security and ICT-enabled economic development in order to explore possible strategies for desecuritization (Flick, 2014).

Whilst the scope is limited to the desecuritization of ICT development, the many proponents of adaptation that have to occur of state functions, business, and individuals would be limited by fixed categorization. By applying thematic approach, when interviewing and interpreting data

collected, discursively, allows us to explore avenues for China and Tanzania to desecuritize issues arising from ICT development. The exploratory nature of the study encourages a structure that is not rigid as we lack basis in the form of previous research about the concerns and opportunities Tanzanians perceive regarding China and ICT development, and this is representative in interviewees' responses. Hence, attaining narratives to further discern themes that can be applied for further contextualizing means to alleviate security issues (Esser & Vliegenthart, 2017).

Additionally, when applying qualitative narrative analysis, the data collected ought to be comparable across contexts, as these methodological boundaries applied with accuracy are invaluable to the field of international relations especially relating to qualitative discourse analysis, as otherwise validity is diminished (Thies, 2002). As such, qualitative narrative analysis is applied to extract themes and sentiments for conceptual categorization, thus fostering greater generalizability, pursuant of imbuing broader discourse in regards to pre-emptive desecuritization in the ICT sector for developing countries, within a stringent theoretical and methodological framework. (Della & Keating, 2008). Wherein the securitization theorist is freed from the ties of securitization theory (i.e. merely observing what is going on), [y] as it is here where the analyst can be political and argue either for or against an incidence of securitization (Wæver, 2015).

3.5 Data Selection

The choice of data is informed by the exploratory nature of study, arising from a desire to move beyond discourse regarding Chinese versus Western geopolitical dominance in Africa, extraction of resources etc. (Downing, 2018). Rather a discursive approach to explore a how amidst a global rush to learn how to govern threats arising from increased connectivity, how do African states who are still relatively young and severely lagging in their ICT adaptation, preempt issues of lagging data protection, technological literacy and outsourcing. This informed the decision to use interviews conducted within the theoretical framework of (De)securitization and diplomacy. By doing so the process is structured yet no to the point where the researchers' biases become apparent, permitting for narrative responses that can be explored after to detect themes (Brinkmann & Kvale, 2018).

To support the finding from interviewers the discursive discussed alongside document reviewed, ranging from policy statements, legislature, and articles, this is in order to juxtapose perspectives, narratives and institutional practices, within the capacity building and desecuritization context (Esser & Vliegenthart, 2017)

As such instead of interviews and narratives, looking at state initiatives, distribution mediums, and applications of soft power, as means to understand how the state apparatus of both China and its Sub-Saharan partners address or preempt security issues (Matthes, 2011). By first conducting interviews and collecting policy agendas and statements from Tanzania, to distill themes, then proceed to discursively compare and explore data representative of China and other Sub-Saharan operational mode application of soft power in the forming of ICT technologies corporation. Meaning identifying data that includes recurring patterns within stakeholder statements, existing literature state initiatives and diplomatic efforts (Esser & Vliegenhart, 2017).

Upon identifying gaps, correlations as well as unforeseen themes, conceptuality within securitization theory as well as capacity building efforts, the final part of the analysis discerns findings solely to contextualize opportunities for “functional ICT cooperation” in the China and Tanzania case, and the degree of the findings’ generalizability.

4. Analysis

Departing from the theoretical assumption that state issues are not essentially security threats unless framed, this section explores interviews, literature, review and policy statements in a discourse framed within desecuritization, in order to contextualize how security concerns…"are reversed and issues are moved out of '...the threat — defense sequence and into the ordinary public sphere' where they can be dealt with in accordance with the rules of the (democratic) political system" (Taurek, p.56 2006). As such, within our interpretivist research design and constructivist scientific approach, the current analysis distills themes and is conceptualizing narratives in relation to the core components of securitization theory in (Della & Keating, 2008).

4.1 Securitization Components of Sino-Tanzanian Relations

In the theoretical framework chosen for the current study, the **Existential Threat includes the variety of political and geopolitical sentiments surrounding the increased influence of Chinese ICT actors. This threat has two security layers;**

(1) Fear of overdependence on China for information management and ICT-enabled services in the long run;

(2) Potential threats of upending political landscape in the country by utilizing cyber-space techniques (disruptions, data leaks, interferences)

These concerns are further reflected in the overarching narrative surrounding the intersection of Huawei in China-Africa bilateral arrangements, especially due to the centralization that has occurred between ICT infrastructure, cybersecurity, national security, and business flow, and considerable the opportunity of data manipulation and sharing between the Chinese and African governments that can be deployed to suppress dissent in the hands of potentially authoritarian regimes (Noesselt, 2019). Respondents varied in the significance and comprehension of the severity of the threats arising from adaptation of emerging technologies, due to variation in digital literacy. A common theme was placing responsibility on politicians to legislate adequately and concern that lack of digital utility and understanding amongst the general populace posed security threats to the state functions and the private sector.

"a need for a stronger, broader understanding amongst Government and policy-makers on what cyber security means and what threats are out there."

"...fear as cyber security is quite an expensive thing to maintain, Tanzania may not financially capable to maintain and in turn will turn to a lender for support which leads to further debt and lack of control of the local security systems"

The above quotes from the interview responses reflect the most commonly recurring themes regarding external threats. Most fear of over dependency not only on China but the West. Additional respondents voiced a concern for lack of digital literacy leaving all parties from state to person vulnerable to data breaches and interference.

"Most Tanzanians are not well-educated or well-informed about the new technology and its risks. So if the organization's do not have good investment in cybersecurity control, this can lead to lacking of sufficient cybersecurity protections and the ability to prevent and control cyber threats to private people"

Whilst this was a limited concern thematic amongst respondents, we attribute this to perhaps lack of awareness and digital literacy amongst respondents, hence a lack of comprehension as to severity and expansiveness of cybercrime. This assumption is not solely based upon a low the usage rate of digital infrastructure, as displayed by Okeleke (2018), or Tanzania's low ranking in HDI (UNDP, 2020); it has to do with the overarching narrative concerning the disruptive force of digitization, that most but a few do not possess the digital literacy to adequately govern this space. This ought to be kept in mind when conducting interviews regarding ICT development in countries with low proliferation of technologies and large social stratification.

In our interview responses, only 1 respondent out of the sample indicated that the Tanzanian-Chinese relations are not threatened by the possible security concerns and over-dependence on China. Employing the sentiment text analysis, summarized in Table 4, we can identify the most important aspects of the relationship for the target audience. In line with broader media narratives (and in contrast to political evidence and latest dynamics in the partnership between countries), Tanzania is perceived by the general public as the political side displaying a position of weakness and "relinquishment". Importantly, when mentioning Tanzania's position of

weakness, respondents would often (58.8%) indicate that Tanzania is generally weak geopolitically not only to China but "to many countries". In line with the discussion in Section 1 and Section 2, corporations' influence is overshadowing the theme of Chinese political interests and the broader perspective over the state of ICT in the country.

Theme	Recurrence (% of responses)
Tanzania's position of weakness	68
Vulnerability of Infrastructure	60
Corporations Influence (Huawei)	40
Political Interest	32
Gap in ICT Development between China and Tanzania	32

Table 4. Recurrence of themes in Interview Responses "Do you think Tanzania is vulnerable to China's long-term influence"

The comments provided in the interviews do not stray too far from other common narratives regarding the supposed Huawei data breach at the African Union headquarters, which was made possible due to the centralization and intersection of security tools and private devices (Shoebridge, 2018). Another existential threat that arises from within, due to centralization of ICT infrastructure is the suppression of any dissent. Whilst this theme is a common narrative about Tanzania digital regulatory framework, especially in light of the 2020 election, accompanied with social media outages and government surveillance (Allen & Kelly, 2022), no respondents voiced concern for this. In fact, most viewed the government's cyber security regulatory framework in a positive light. This can be prescribed to many factors, one being fear as many will not speak ill of the government in digital or public domains, however many Tanzanians viewed now deceased President John Magufuli as a strong leader willing to stand up to the West and China, showcased by the extensive delays in the Bagamoyo port project.

The divergence in sentiments regarding the fears underlying the Existential Threat component within the interview answers are summarized in the text cloud below (Graph 9). As per the interview design the question "*How do you perceive Tanzania's readiness to adapt new technologies and increased connectivity i.e., cyber security?"* was framed in the generic way in order to understand the overall direction of the thinking the sample respondents have when it comes to these threats. In contrast to the trends described in the theoretical framework and recent developments in cyber-security area, a notable distinction of the interview findings lies in still high importance that respondents ascribed to a much simpler technique of cyber security – *scamming, fraud, hackings into private banking information.* This indicates that in contrast to general media narratives presented, which are largely focused on more politicized components of cyber security in Tanzania, the concerns of the users largely lie within last-generation cyber crimes, and lack of digital culture.

Graph 9. TextCloud of "Fears in terms of Tanzania's readiness to adapt new technologies". The size of the word corresponds to the recurrence. The Themes are grouped thematically.

As such, we transition to uncovering the **Securitizing Actor component which encompasses the Tanzanian government and public sector officials.** As we explored in Section 1, Tanzanian regulatory framework has undergone a transformation over the last 2 decades with a significant centralization of power into the hands of the Ministry of Work, Science and Technology for strategic decision-making and TCRA for legislative framework. Therefore, we limit our exploration to the impact of actions, statements, public speeches, laws, and regulations enforced by the central government of Tanzania.

A case in point that underlines the role of securitizing actor is The Law Reform Commission of Tanzania with its acknowledgement that current laws governing cyberspace not being legislatively distinct enough protect against cyber-crimes, and thus they sets forth an intention to further study how to properly legislate this space, in order to encourage commerce (Kato, 2019). A year prior Tanzania passed its "landmark" cybercrimes act, and to our surprise, interviewed consistently touted the government for its strong stance on cybersecurity.

> *"For the government of Tanzania, it has shown much effort really in protecting such situations to the face of the citizen because there are laws that a introduced so that to protect and guide well the issue of cyber attacks. A good example is our President or should I say the former President Mr Jakaya Kikwete who introduced laws that could govern our country Tanzania and Zanzibar in one way or another. The Law further criminalizes and penalizes a number of cyber activities such as data espionage, publication of child pornography, publication of pornography, publication of false, deceptive, misleading or inaccurate information, production and dissemination of racist and xenophobic material, initiating transmission of or re-transmission of unsolicited messages and violation of intellectual property rights and other types of cybercrimes."*

It is noteworthy that none of the interviewed expressed direct concern regarding recurring themes expressed in discourse preceding, as to the use of surveillance and media outages to suppress opposition, especially given that respondents directly experienced it in Tanzania's 2020 election. Which is in line as previously stated Tanzanians have a high level of trust in governance

(Okeleke, 2018). The recurring sentiment amongst interviewed subjects deviates from the scrutiny the Cyber Crimes Act has gotten respective to its empowerment of law enforcement and application to suppress opposition (Allen & Kelly, 2022).

Within the context of desecuritization and Tanzanian government being the securitizing actor, the policy statements and legislative action indicate relative awareness or an attempt to alleviate fears by bringing the discourse to the public sphere, and seeking to employ policies and regulations to diminish or rebrand Cyber crimes (Burton & Lain, 2020). Why Tanzania shows a lack of concern as to the empowerment of law enforcement within cyberspace begs for further exploration. Means of addressing existential threats for the Tanzanian business sector, however, are diminished due to lack of autonomy. This is due to the nature of bilateral cooperation by way of reciprocity between China, Tanzania, and Huawei. Arrangements between private sector and state. Representative of an intentional strategic initiative emphasized again by the *Ministry of Foreign Affairs of China in 2021,* in order to foster long-term cooperation between China and Africa. This poses a concern for Tanzania as a securitizing actor, that we ensure to explore. At various times within interviews a common theme of cognitive dissonance arose reflecting apprehension and willingness towards Chinese influence. Perhaps a reflection of the loaded development practice being a necessity at too too steep a price.

> *"Tanzania and China can come together in a partnership that will be mutually beneficial and not one that will see Tanzania crippled with debt and a lack of autonomous control of the countries security systems"*

In this light, President Magufuli was much applauded for applying both legislative framework and a continuous public narrative that was directly aimed at China. Such deeds included the delaying of the Bagamoyo Port construction agreement 5 to 7 years, as well as travel restriction on civil servants that constricted capacity efforts. Further expounded by the former President Magufuli stating that …"*Chinese investors are coming with tough conditions that can only be accepted by mad people"* (M'bwana, 2019). Displaying a strong stance towards China publicly within our

theoretical framework can be considered a mode of applying narratives to reframe a matter to alleviate the theme of lack of autonomy as the Securitizing Actor.

This statement was made specifically in regard to the Bagamoyo port deal that was signed prior to President Magufuli taking office (M'bwana, 2019). This is partially the reason many Tanzanians took a liking to him, as he was consistent in his hard stance towards foreign investors and development projects. The delaying of the Bagamoyo Port agreement, coupled with the legislative measures limiting civil servants travel from China, as well as a consistent public stance against foreign investment, distilled within desecuritization, is the application of both narrative and institutional practices deployed within the public space to reframe or diminish tension, intentionally or not is beyond the scope (Buzan & Wæver 2003). It is never that simple however, as misinformation and opposing narratives arise, the ability to draw correlations is hardened. We can take for example 2019 the former statement as to those willing to accept Chinese terms being "mad men", comparative to President Magufuli's position in 2021, when meeting with Chinese Foreign Minister Wang Yi in Chato… *"Tanzania is ready to deepen cooperation with China…attract more Chinese investment. Tanzania is ready to become the gateway for Chinese enterprises to explore the eastern and southern African markets…"* (Embassy of The People's Republic of China, 2021). This presents confusion, and interviews did voice concerns as to misinformation as well as makes it difficult what role Tanzania is taking as a securitizing actor, especially in light of opposition suppression in 2020. Combining this with strategic capacity efforts China employs in Africa, as Tang argues, it can be inferred that the transference of knowledge is thus conducted via Chinese Tech giants and started to have a significant impact on the audience and Securitizing Actor (Tang, 2021).

4.3 Desecuritizing ICT to Unlock Growth through Capacity Building

Applying capacity-building as desecuritizing means, therefore time is spent looking at devices and actions that accompany capacity building efforts, within securitization theory we discern the role of audience, rhetorical devices and emergency actions.

When discussing **Audience component of securitization** in the African context access is often limited to narrow elite circles not the general public of the country (Ezeokafor & Kaunert, 2018) Considered relative to the process of discretization the role of the referent audience has a significant influence on the securitization process, which begs the question, what role do the narrow elites play in this process relative to the public with limited access to information (Buzan & Wæver 2003). Upon reflecting on their own role, a persistent narrative emerged within interviews insistent on education, as well as an openness or understanding of the necessity for China Tanzania ICT partnership.

> *"Citizens should be informed about the risks they all face and the steps they can take to stay secure. Improving ICT education and information"*
>
> *"It's a good thing for the Tanzanians to gain new skills, knowledge, education, this can contribute to economic growth of the country"*

This is in sync with desecuritization being a process that education, awareness and capacity development are inline, and the audience's responsiveness is encouraging towards functional cooperation (Burton & Lain, 2020). Despite audience willingness there is still a severe lag in the private sectors adaptation of ICT infrastructure (UNCTAD, 2020). This correlates casually to interviews assertion, that the sudden flood of new technologies into Africa without the necessary digital literacy being a component of the slow transition. Yet the audience may be considered part of the elite or at least those with access, and this is a gap within the study, as to proper sampling. However, it does reflect that an appeal exists garnered through rhetorical mediums.

There is an evident eagerness prevalent amongst interviewees especially the younger as to the potential ICT brings in terms of innovative development, which despite the small sample size is in cohort with narratives and plans set for by the Tanzanian government outlining the

liberalization of ICT development in order to promote innovation (Tanzania Development Vision 2025).

Given that the referent object intersection between state individual and business, reflective initiative shows however an effort to deploy legislative and institutional devices to foster appeal. Stakeholder appeal is further supplanted by Chinese strategic efforts to couple investment with transference of technological competencies (Tang, 2015). Nevertheless, the confluence of actors employing rhetorical devices to garner appeal, engenders concerns about who is outlining strategies? Shi discuss concerning narratives regarding big tech companies being the major forces shaping ICT development in Africa (Shi, 2019). Utopian functionality is not the end game, and many studies have focused on the net gains versus losses in relations between countries in the global south and north, as such all that can be explored is what institutional practices can diminish risks arising from ICT adaptation dependency. One such mitigating factor reflective across the board in interview responses is education and training empowering self-governance which leads us into the next aspect of analysis.

> *"When it comes to the situation of self-employment most of Tanzanians do not have that accessibility of doing most of the things but through the knowledge they give via ICT it gives mostly youth the ability to do and create much impacts on making a greater step of what they truly can do. Knowledge is knowledge and the power"*
>
> *"On education level such as online education, tutorials. New job opportunities, flexible , mobile working, network, ways for people to interact"*
>
> *"Even the flood of new technologies is transference of knowledge"*

Whether this eagerness due to such plans as the Tanzania Development Vision 2025 or the mere access to opportunities the responses reflect responsiveness despite previous observation of the triangulation of securitizing actors that include China, Big Tech (Polyakova & Meserole, 2019). Does that mean Tanzania has had relative success with emergency action targeted at diminishing initial rejection? Given the necessity for immediate education expressed, and the gap it creates between technology availability and usage, the current model that encourages bilateral agreements, and Chinese capacity building efforts at the risk of leaving ideological footprints, is perhaps the best option for states with lesser economies (Blanchard & Flint,

2017). The nuanced approach by former president Magfuli as appealing tough on China whilst still placating is perhaps a proponent of alleviating fear of Chinese intrusion (M'bwana, 2019).

However, with that predisposition further exploration ought to be given to how to mitigate fears of authoritarian footprints, which brings us back to overarching concerns subjects of potentially authoritarian regimes such as Tanzania live with (Cavelty, 2020). Thus, questions arise as to the individual empowerment due to the disruptive power of the internet and the function it plays within a developing potentially authoritarian state.

Given our attained understanding of themes that concern Tanzanians in the context of desecuritization components, we proceed to consider the framing of ICT development between China and Tanzania relative to other East African countries. This is done in order to find correlations and deviations that may be applicable to Tanzania's case as a country in its early stages of ICT development.

4.4 Desecuritization: Challenges and Opportunities

Having inferred the recurrent themes from the interview analysis such as capacity building-related issues that overshadowed the politicized components – education, digital literacy to properly govern cyberspace, and access as the main concerns facing Tanzanians interviewed, the following section reflects on challenges and opportunities in this direction. As such the discourse is reconnected to recent **discussed in the Section 1.3** as well as research, development and capacity building efforts in the East African region.

Other East African countries have shown a propensity to adapt the Chinese legal and regulatory model, as discussed within the literature review, one needs only look to Ethiopia total control of data governance (Polyakova & Meserole, 2019). Uganda has experienced similar issues, with the regulatory frameworks permitting the suppression of opposition (Noesselt, 2019). This does not differ too much to the Tanzanian experience prior to the death of later President Magufuli, who whilst praised for his hard stance on China, implemented via the TCRA's several amendments

limiting and constricting data and flow of information, especially from incoming from other countries. As we have previously determined much has already been said about China's soft power in Africa, and the possible fear of authoritarian tendencies accompanying capacity building.

Yet from a desecuritization perspective, what is noteworthy is the departure from policy statements to the instruments and institutions that uphold them notwithstanding. Partially this can be due to the unaccountable variable of change in leadership as well as authoritarian tendencies in developing countries. This presents a prevailing problem for intersubjective cooperation between the Tanzanian state and it's citizen fostering decuritizing measures and institutions without the interference of Chinese soft power (Polyakova & Meserole, 2019; Sanahuja, 2021) .This is a cost, that there is a seeming willingness to pay due to the necessity for knowledge transference, which was reflected especially amongst young interviewees, due to the preceptive innovative possibilities accompanied by decentralized knowledge exchange (Burton & Lain, 2020). Therefore, Tanzania has proven to be not capable of framing the issue alone, and the legal and regulatory mechanisms applied to frame ICT adaptation are due to necessity impacted by Big Tech companies who set forth implementation strategies, and in Tanzania regard those are Huawei and ZTE (Shi, 2019). This further intersects with the Capacity building framing, as part of Huawei's plan in Africa is to engender long-standing relationships, via long-term deals, and skills and knowledge transference, in order to bolster ICT infrastructure (Mingliang, 2021). This again highlights the concern that Chinese traditions are being passed along as part of the transference of skills and knowledge, and such are becoming framers of development.

Juxtaposing modes of desecuritization across East African countries and Tanzania, it stands out by the higher trust in central governance. The high trust is garnered in recent years due to being the country displaying most discontent and skepticism publicly towards both China and Western partners (Blanchard, 2020). This is further evident in opting out of the Telecom agreement, the extensive delays with the Bagamoyo port, and limiting travel of civil servants from China (Hoffman 2018; M'bwana, 2019). Nevertheless, as exposed in the results of the interviews, the

general publics' perception is still much more inclined to the narrative of "weakness" and "relinquishment" on the side of Tanzania.

Overregulation is another theme that even overshadowed the topic of the country's vulnerability. Much of the power is concentrated within the centralized model of the Tanzanian telecommunications regulations – from strategic decisions on partnerships with China and Huawei to creating legislative acts that make the transfer of technology very slow across the business actors in the country. The number of respondents indicated high threshold to obtain licenses and as well heavy taxation as challenges that make Tanzanian ICT entrepreneurship "locked in".

> *"There should be a gradual change towards tech but with comprehensive training that all citizens have a basic understanding of what internet security is and in terms of how they can protect themselves and their identity while on the internet."*
>
> *"I would like to see the government invest further in educating local Tanzanian in hopes that we will be better equipped in the near future with skilled individuals as well has full autonomy over local security system"*
>
> *"More education to Tanzanians regarding internet security, the citizens should be informed about the risks they all face and the steps they can to stay secure. Improving lCT education and information"*

There is a disconnect between the policy documents and the findings of our thematic analyses along the lines of **who should take responsibility for desecuritization,** in this particular case, desecuritization through technology transfer from external investors to local actors. Whereas strategic documents such as Tanzania Development Vision 2025 and Digital Strategy Project, Tanzanian government and international non-governmental organizations identified that they should focus on *obliging foreign investors to reinforce infrastructure development and aid with building capacity among Tanzanian citizens.* In contrast to this, the interview respondents overwhelmingly identified the lack of the government's initiative in providing training. Hence, overcoming the dilemma of how to foster future cooperation between Tanzania, China and Huawei to create the environment conducive to knowledge sharing is the major challenge to unlock desecuritization process.

5. Conclusion

In this article, our objective was to explore cooperation between China and Tanzania in the realm of ICT through employing the conventional (de)securitization framework to outline potential national security concerns underpinning this cooperation. Securitization theoretical framework can be applied into Cyber Security framework but only taking into account certain properties of cyber security as a field. For instance, unlike more conventional areas of national security, cybersecurity is characterized by rudimentary phase of legislative and protective frameworks that make it less possible to capture securitization process, identify its direction, and look beyond political decisions.

Resting upon the review of the Sino-Tanzanian ICT cooperation, we identified Existential Threat, Audience, Securitizing Actor, Rhetorical Devices and Plan of Actions by using interview respondents from the public officials, ICT entrepreneurs, and academia specialists in this area. We then reconnected with the current media discourse in Tanzania and public statements from Chinese and Tanzanian officials to identify discrepancies between how the threats are viewed among the end-users and how they are presented in the media. This enables us proposing the technology transfer / capacity-building path as an opportunity for desecuritization.

The findings of this thesis expand the current bulk of research in the area of Securitization in the number of ways. First, we contribute to exploring how Securitization can be applied in a non-Western context. Through narrative analysis and review of the sectoral modes of cooperation, we identified idiosyncrasies of the political and economic agenda in Tanzania that call for re-adjustment of the Copenhagen School Securitization Theory when being applied in the East African context. Thus, in Africa, perception of cyber security is different and reliant on more quotidian aspects of security (fraud, hackings, scam). With higher respect to traditions and hierarchies on the one side, and lower internet proliferation on another, securitization process is different from the West, and is based on elite-to-elite engagement rather than appeal to the broader audience. Finally, the view over interaction between the national governments and the foreign superpowers is still affected by the country's colonial history and this leads to the fact

that Sino-African cooperation cannot escape the public's perceptions where it will be compared to these countries' colonial past, no matter how distant this comparison can be.

More research should be focused on decomposition of the desecuritization process in cyber-security using case studies that involve particular instances of cyber threats in East Africa. Furthermore, concretization of the role of a Desecuritizing Actor, who should take responsibility for desecuritization in the cyber security context can be uncovered in the further research,

References

Afrique, H. (2021, March 18). Ethiopia: Mr Chen Mingliang "Huawei's main investment in the Ethiopia market has been to transfer its know-how". allafrica. other.

Alden, C., Chichava, S., Jiang, L., Murg, B., Lim, G., & Wu, Y. S. (2021). China-Driven Port Development: Lessons from Kenya and Malaysia. *SAIIA Policy Briefing*, (257-290).

Allen, N., & Kelly, C. L. (2022, January 4). Deluge of Digital Repression Threatens African Security. Africacenter.org. African Center for Strategic Studies

Arsène, S. (2013). The Chinese ICT Development Strategy in Africa. Transparency, Sovereignty and Soft power.

Balzacq, T. (2011). Securitization theory. *How Security Problems Emerge and Dissolve (Peace Research Institute Oslo (PRIO)*.

Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), 110-123.

Bilgin, P. (2011). Politics of studying securitization? The Copenhagen School in Turkey. *Security dialogue*, *42* (5), 399-414.

Blanchard, J. M. F. (2020). Problematic prognostications about China's maritime silk road initiative (MSRI): Lessons from Africa and the Middle East. *Journal of Contemporary China*, *29*(122), 159-174.

Blanchard, J. M. F., & Flint, C. (2017). The geopolitics of China's maritime silk road initiative. *Geopolitics*, *22*(2), 223-245.

Bryman, A. (2015). Social Research Methods - 5th Edition. Oxford: OXFORD University Press.

Della, P. D., & Keating, M. (Eds.). (2008). Approaches and methodologies in the social sciences.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

Burton, J., & Christou, G. (2021). Bridging the gap between cyberwar and cyberpeace. *International Affairs*, *97*(6), 1727-1747.

Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, *5*(3), 449-470.

Buzan, B., & Wæver, O. (2003). *Regions and powers: the structure of international security* (Vol. 91). Cambridge University Press.

Buzan, B., Wæver, O. & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Carrozza, I. (2018). China's African Union diplomacy: challenges and prospects for the future.

Cavelty, M. D. (2020). Cybersecurity between hyper-securitization and technological routine. In *Routledge Handbook of International Cybersecurity* (pp. 11-21).

DataReportal (2021). Digital Tanzania 2021. Retrieved from https://datareportal.com/reports/

Downing, K (2018). China's Desire for Soft Power.Leiden University

Dutta, S., & Lanvin, B. (2019). The Network Readiness Index 2019. Washington: Portulans Institute.

Emmel, N. (2013). Theoretical or purposive sampling. In Sampling and choosing cases in qualitative research: A realist approach (pp. 45-66). Retrieved from https://dx.doi.org/10.4135/9781473913882

Esselaar, S., & Adam, L. (2013). Understanding what is Happening in ICT in Tanzania: A Supply-and Demand-side Analysis of the ICT Sector. Retrieved from: https://media.africaportal.org/documents/Policy_Paper_11_-_Understanding_what_is_happening_in_ICT_in_Tanzania.pdf

Esser, F. & Vliegenthart, R. (2017). Comparative research methods. The International Encyclopedia of Communication Research Methods, 1-22. doi:10.1002/9781118901731.iecrm0035

Ezeokafor, E., & Kaunert, C. (2018). Securitization outside of the West: conceptualizing the securitization–neo-patrimonialism nexus in Africa. *Global Discourse*, *8*(1), 83-99.

Flick, U. (2014): An Introduction to Qualitative Research (5th Edition) London: Sage Publications Ltd.

Forje, E. (2018). Unblocking Africa's Underdevelopment Through The One Belt, One Road. *Belt and Road Initiative: Alternative Development Path for Africa*, 7.

Gatere, G. S. (2019). The Impact Of China'S Soft Power Diplomacy On Sustainable Development In Africa (Doctoral dissertation, University of Nairobi).

Gupta, V. (2020). A Case Study on Economic Development of Tanzania. Journal of the International Academy for Case Studies, 26 (1).

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Hanusch, M. (2012). African perspectives on China–Africa: Modelling popular perceptions and their economic and political determinants. *Oxford Development Studies*, *40*(4), 492-516.

Hoffman, A. (2018). Africa Telecommunications Infrastructure in 2018: Overview and Policy Recommendations. Available at SSRN 3265849.

Hönke, J. (2018). Port geographies: Africa's infrastructure boom and the reconfiguration of power and authority. In *Extractive Industries and Changing State Dynamics in Africa* (pp. 41-56). Routledge.

Huawei Annual Report. (2020).Huawei Annual Report: Seeds for The Future Programme. Retreivied from Huawei.com

Hunt, E. F., & Colander, D. C. (2017). Social science: An introduction to the study of society.

IEA. (2021). Access to Electricity: Data and Projections. Retrieved from https://www.iea.org/reports/sdg7-data-and-projections/access-to-electricity

Jackson, R., Sørensen, G., & Møller, J. (2018-12-13). Introduction to International Relations: Theories and Approaches. Oxford: Oxford University Press.

Jamshed S. (2014). Qualitative research method-interviewing and observation. Journal of basic and clinical pharmacy, 5(4), 87–88. https://doi.org/10.4103/0976-0105.141942

Johnson, K. R. (2018). Viability of Shared Mobile Network Infrastructure in Tanzania (Doctoral dissertation, College of Business Education).

Kasper, A. (2014). The fragmented securitization of cyber threats. In *Regulating eTechnologies in the European Union* (pp. 157-187). Springer, Cham.

Kato, C. I. (2019). Legal framework challenges to e-banking in Tanzania. *PSU Research Review.*

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100-115.

Makundi, H., Huyse, H., & Develtere, P. (2017). Negotiating the technological capacity in Chinese engagements: Is the Tanzanian government in the driving seat?. *South African Journal of International Affairs*, *24*(3), 331-353.

M'bwana, L. (2019, December 28). "Only mad people accept Chinese deals"- chides Tanzanian President Magufuli. Maravipost. Retrieved from https://www.maravipost.com/only-mad-people-accept-chinese-deals-chides-tanzanian-president-magufuli/.

Ministry of Foreign Affairs of China. (2021). Forum on China-Africa Cooperation Dakar Action Plan (2022-2024). Retrieved from: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202112/t20211202_10461183.html

Monson, J. (2013). Remembering work on the Tazara railway in Africa and China, 1965–2011: When "New Men" grow old. *African Studies Review*, *56*(1), 45-64.

Mpambije, C. J. (2021). Leveraging the Roles and Constraints in Enhancing Industrialization in Tanzania. Tanzania Journal of Development Studies, 19.

Mukwaya, R., & Mold, A. (2018, December). Modelling the economic impact of the China Belt and Road Initiative on East Africa. In *African Economic Conference. Kigali* (pp. 3-5).

Ndung'u, N. (2019). Digital technology and state capacity in Kenya. Washington, DC.

Network Readiness Index Report. (2021). Benchmarking the future of the digital economy. Findings and Data Overview. 31-90.

Network Readiness Index. (2021). Country Profile – Tanzania. Retrieved from https://networkreadinessindex.org/country/tanzania/

Noesselt, N. (2019). China's African dream: Assessing China's new strategy. In *China's New Role in African Politics* (pp. 17-31). Routledge.

Nye, J. S. (2012). China and soft power. South African Journal of International Affairs, 19(2), 151–155. doi: 10.1080/10220461.2012.706889

Nyman, J. (2013). Securitization theory. In *Critical approaches to security* (pp. 66-77). Routledge.

Okeleke, K. (2018). GSMA: Digital transformation in Tanzania The role of mobile technology and impact on development goals. Retrieved from: https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=39256224&file=2736-180319-Tanzania.pdf

Ortiz-Crespo, B., Steinke, J., Quirós, C. F., van de Gevel, J., Daudi, H., Gaspar Mgimiloko, M., & van Etten, J. (2020). User-centred design of a digital advisory service: Enhancing public agricultural extension for sustainable intensification in Tanzania. *International journal of agricultural sustainability*, 1-17.

Parks, L., & Thompson, R. (2020). Internet Shutdown in Africa, The Slow Shutdown: Information and Internet Regulation in Tanzania and Impacts on Online Content. International Journal of Communication, 14, 21.

Parks, L., Srinivasan, R., & Aragon, D. C. (2021). Digital empowerment for whom? An analysis of 'Network sovereignty'in low-income, rural communities in Mexico and Tanzania. *Information, Communication & Society*, 1-22.

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series (Washington, DC: Brookings, 2019)*, 1-22.

Sanahuja, J. A. (2021). The Copenhagen School: the (de) securitization of UNASUR (2008-2017). International Politics l, 64.

Sen, G., & Bingqin, L. (2019). The Digital Silk Road and the sustainable development goals (SDGs). *IDS Bulletin*

Shi, X. (2019). *China's foreign aid in East Africa: Decentralising cooperation* (Doctoral dissertation, [Sl: sn]).

Shoebridge, M. (2018). Chinese cyber espionage and the national security risks Huawei poses to 5G networks. Macdonald-Laurier Institute for Public Policy.

Sitnicki, M., & Netreba, I. (2020). Inter-dependence assessment for Network Readiness Index. Baltic Journal of Economic Studies, 6(2), 47-53.

Stein, H. (2019). Economic policy and the IMF in Tanzania: Conditionality, conflict, and convergence. In *Tanzania and the IMF* (pp. 59-83). Routledge.

Tang, Y. (2021). The Operations of Chinese Infrastructure Multinationals in Africa. *Springer Books*.

Tanzanian Communications Regulatory Authority (2021). Data Sheet – Digital Tanzania Project. https://www.tcra.go.tz/

Taureck, R. Securitization theory and securitization studies. J Int Relat Dev 9, 53–61 (2006). https://doi.org/10.1057/palgrave.jird.1800072

The World Bank. (2016). World development report 2016: digital dividends. World Bank Publications.

The World Bank. (2021a). Gross Domestic Product, % Growth Rate.

The World Bank. (2021b). Share of Population Having Access to Grid Electricity.

The World Bank. (2021c). Individuals daily accessing Internet (% of total population).

Thies, C.G. (2002). A pragmatic guide to qualitative historical analysis in the study of international relations. International Studies Perspectives, 3, 351-372.

UNCTAD (2020). United Republic of Tanzania Rapid eTrade Readiness Assessment. Retrieved from:

UNDP (2020). Latest Human Development Index. Retrieved from http://hdr.undp.org/en/content/latest-human-development-index-ranking

UNESCO (2020). Country Profile Statistics – Tanzania. Education Enrollment and Attainment. Retrieved from: http://uis.unesco.org/country/TZ

van Giezen, A., Eggers, L., Peters, A., & Prasad, R. (2021). Do the Chinese bring Sustainable Development to Africa? The Silk Road and the Port of Bagamoyo in Tanzania. *Out of China: Responsible Port Innovation along the 21st Century Maritime Silk Road*, 131.

Wendt, Alexander. (1992) 'Anarchy is What States Make of It: The Social Construction of Power Politics', International Organization 46(2): 391–425.

Wæver, O. (1993). *Securitization and desecuritization* (p. 48). Copenhagen: Centre for Peace and Conflict Research.

Wæver, O. (2015). The theory act: Responsibility and exactitude as seen from securitization. *International Relations*, *29*(1), 121-127.

White, T. (2020). China's Indian Ocean Ambitions: Investment, Influence, and Military Advantage. Brookings. Retrieved from https://www.brookings.edu/wp-content/uploads/2020/06/FP_20200615_chinas_indian_ocean_ambitions_white-1.pdf

Wilkinson, C. (2007). The Copenhagen School on Tour in Kyrgyzstan: Is securitization theory Useable outside Europe? *Security dialogue*, *38*(1), 5-25.

Wong, P. (2021). *Techno-Geopolitics: US-China Tech War and the practice of digital statecraft*. Routledge India.

Xing, Z. (2018). The impacts of Information and Communications Technology (ICT) and E-commerce on bilateral trade flows. I*nternational Economics and Economic Policy, 15(3), 565-586.*

Zaamout, N., Alton, T., & Houlden, G. (2019). Examining Huawei's Growth & Global Reach: Key Implications, Issues, and the Canadian Connection.

Zhang, X., Wasserman, H., & Mano, W. (Eds.). (2016). China's media and soft power in Africa: promotion and perceptions. Springer.

Appendix A. Interview Questions (Semi-Structured)

Are you a Local Tanzanian or an Expat?
Age?
What is your highest level of education?
What positives have you seen from Tanzania's improved ICT technologies and increased connectivity?
How do you perceive Tanzania's readiness to adapt new technologies and increased connectivity i.e., cyber security?"
How do you see the governments readiness for to protect Tanzanian citizens against cyber attacks ?
Does the government invest enough in research and development projects in technology in your opinion?
How do you view China's effort training, teaching and transferring knowledge to Tanzanian?
Do you think Tanzania is vulnerable to China considering the ICT infrastructure developments?
What would you like to see the Tanzanian government do to prepare Tanzania in terms of internet security?
How can China and Tanzania work together so both countries benefit from their relationship in the ICT technologies sector?