"The Coloniality of Chinese Surveillance Technologies in Africa"

Sakarombe Erick, Chimwamurombe Fannuel, Masuku Sandisiwe Sukoluhle, Mupanga James and Mutume Tanaka Elspet Cordelia

University of Zimbabwe

DOI: https://dx.doi.org/10.47772/IJRISS.2025.9020107

Received: 24 January 2025; Accepted: 29 January 2025; Published: 05 March 2025

ABSTRACT

This paper explores the implications of Chinese surveillance technologies in Africa, positioning the discussion within the framework of digital colonialism. As African nations increasingly implement advanced surveillance systems developed by Chinese firms, significant concerns emerge regarding the erosion of civil liberties and the entrenchment of authoritarian governance. Technologies such as facial recognition and data analytics, often marketed as enhancements for public safety, have been exploited by various regimes to monitor dissent and suppress opposition, reflecting historical patterns of colonial control. The research highlights the neo-colonial dynamics at play, where economic dependencies on Chinese technology create a complex interplay of power that undermines local autonomy. Although proponents argue that these technologies foster economic development, the reality reveals a troubling trend of illiberal practices and societal surveillance reminiscent of past colonial structures. Through a qualitative analysis of secondary data, including academic literature, legal documents, and media reports, the study emphasizes the urgent need for robust regulatory frameworks to safeguard citizen rights and promote local agency in technology governance. Furthermore, it advocates for a reevaluation of international partnerships, urging African nations to prioritize ethical considerations and local development needs over foreign interests. Ultimately, this paper contributes to the discourse on digital sovereignty and human rights, calling for a collective commitment among African states to assert their technological futures in the face of external pressures, thereby fostering a model of development that is inclusive and rights-respecting.

Keywords: surveillance technologies, digital colonialism, artificial intelligence, population monitoring, authoritarian control, dissent suppression, sustainable development, illiberal practices

INTRODUCTION

China's export of surveillance technologies to African nations has sparked concerns over a new form of digital colonialism emerging on the continent. At the core of this critique is the proliferation of Chinese-developed safe city/smart city platforms that integrate facial recognition, video analytics, mobile tracking and data fusion capabilities into centralized command centers. Companies like Huawei, Hikvision, Dahua, and CloudWalk are major suppliers of these artificial intelligence-powered systems, which enable expansive population monitoring and profiling under the guise of enhancing public safety and security. However, human rights groups allege that African governments have embraced these technologies as tools for entrenching authoritarian control, suppressing dissent, and surveilling opposition groups, journalists, and minority populations. With lax data protection laws, there are risks of privacy infringements and the extraction and monetization of civilian data by Chinese firms. China has framed its technological engagement as a pragmatic partnership among developing nations, casting the technologies as instruments for sustainable development and economic modernization. Yet this perspective arguably downplays concerns around mass surveillance, social control, and citizens' diminishing ability to hold authorities accountable in an era of AI-powered policing. Critics view the coloniality of Chinese surveillance technologies as an erosion of digital freedoms and self-determination in African societies, enabling illiberal practices and hierarchical power structures

reminiscent of historical colonialism. This raises fundamental questions around responsible technological development, data governance, and more rights-respecting models that align with African nations' long-term interests.

BACKGROUND

The paper critically examines the intersection of China's technological expansion and the enduring legacy of colonialism on the African continent. This analysis is situated within a historical framework that highlights how colonial powers established systems of control and exploitation, which have evolved into contemporary forms of digital governance. The increasing reliance of African nations on Chinese surveillance technologies, such as facial recognition systems and data analytics, raises significant concerns about sovereignty and autonomy (Doshi et al., 2021). Scholars argue that this reliance mirrors colonial dynamics, where external powers impose their technologies and governance models, often disregarding local contexts and needs (Chen, 2016; Swedlund, 2017; Langan, 2017). The article posits that the adoption of these technologies is not merely a technical upgrade but a complex interplay of power relations that perpetuates a form of neo-colonialism, where African states may inadvertently cede control over their own governance to foreign entities (Alden, 2007; Reeves, 2018; Balasubramanyam, 2015). China, one of the global superpowers has been making serious inroads in the field of technological investments in Africa. According to Inkster (2018), China is making a sustained effort to become a 'cyber superpower'. Part of the Chinese digital growth is being driven by what Cheung (2018;23) calls the notion of 'internet sovereignty', which implies China's supreme right to govern the internet within its borders and keep it under rigid control.

The digital age has been lauded as very progressive and an integral part of the modern day society. Scholars such as Gravett (2020) have noted that the digital drive has enhanced several facets of the modern society, which includes, inter-alia, access to health, education and economic advancement. In the field of human rights, digital technology has been said to enhance equitable access to justice, democracy and human rights. According to Yuen (2015), principles such as "freedom", "openness", and "interoperability" are critical in the liberal-democratic approach, which assumes that increased internet coverage across countries and the globe support free speech and has the capacity to enhance globalization. The digital growth in China has been massive, spawned by years of significant funding of state owned and private led entities that work in collaboration with the state and the Communist Party.

Sun and Yan, (2020) note that the growth in digital technology in China and internet optimist salivating on the imagined predictions that it will directly result in the weakening grip on the Chinese state. However, the state has increased its surveillance capabilities, where state censorship has gone a notch up. Instead of the internet being a tool for advancing freedoms and human rights, it has resulted in the opposite, where targeting of perceived dissidents has become entrenched in the Chinese state (Hicks, 2022). For instance, the alleged concentration camps of the Uighur Muslims are said to be ridden with advanced technologies that aid in their total subjugation. Far from igniting a political transformation in China the internet is an indispensable tool advancing state censorship and surveillance. China discovered how to exploit the internet and information technology in ways that reduce, instead of enhancing freedom.

China's state surveillance capabilities have developed rapidly and extensively in the 21st century. Gravett (2020) highlights how the Chinese state has expanded its capabilities to sensor free speech and infringe upon the very basic human rights. Of particular note is how China has become the first digital authoritarian state (Jili, 2022). 'Digital authoritarianism' refers to the use of digital information technology by authoritarian regimes to surveil, repress and manipulate domestic and foreign populations. The Chinese have long pioneered digital tools for domestic censorship and surveillance, harking back to the launch of the digital bulwark of Chinese information control, the so called 'Great Firewall' of China, more than two decades ago. Under President Xi Jinping the Chinese government has vastly expanded domestic surveillance to play a greater role in strengthening the Communist Party's hold on society. Rapid advances in surveillance technology, coupled with growing police access to user data, have turned China into a 'techno-dystopia' and have helped facilitate the prosecution of prominent human rights advocates and ordinary users. More content is considered sensitive and activists and journalists are receiving heavy penalties for their online activities. Ethnic and religious

minorities continue to be mercilessly surveilled and persecuted for their spiritual and cultural expression or for exposing human rights abuses against their communities.

The consumption of surveillance technologies in china has led to a new version of the ‘race in manufacturing companies focusing on producing these technologies. Firms such as Hikvision, Huawei and Dahua have expanded rapidly, amongst a host of new ones, offering cutting edge surveillance technologies to the Chinese state. However, domestic demand has been extensively met and therefore, these technologies are now being exported to African countries. Germanò et al., (2023) assert that the Chinese state has exported its surveillance blueprint to African nations with populations that are far less that its own 1 400 000 000. Therefore, it goes that if China has the capacity to monitor such a massive population, African states such as Zimbabwe and Ethiopia can also do the same in the context of significantly smaller populations.

China has been selling its blueprint abroad, including the hardware and software it uses in its surveillance regime. This blueprint is suffused with the potential for developing surveillance societies in China's image, particularly in countries with poor human rights records, where democratic institutions are either weak or still in their infancy. Moreover, as China makes further advances in information technology, this may yield even greater repression, rather than liberalisation, in Africa. Gravett (2023) argues that Chinese technological penetration in Africa raises the spectre of ‘digital neocolonialism’ – the application by China of economic and political pressures, through technology, to control and influence African nations. China has become the world's biggest market for security and surveillance technology.20 By 2010 Beijing alone was blanketed by 800,000 surveillance cameras, and by 2015 Beijing police boasted that the city was 100 per cent covered. In 2015 the government set itself the goal of covering all public spaces and leading industries in 300,000,000 cameras by 2020, with the aim of creating an ‘omnipresent, fully networked, always working and fully controllable’ surveillance system, a nationwide panopticon, combining data mining with sophisticated video and image analysis.

LITERATURE REVIEW

China has built what has been termed as the perfect surveillance state. This ‘Sharp Eyes’ (‘Xue Liang’) initiative is extraordinary for its reach and scope (Velghe, 2019). The name of the project is taken from the Communist slogan ‘the masses have sharp eyes’, and is a throwback to Mao Zedong's attempt to coerce every citizen to spy on others. As ‘Sharp Eyes’ feeds are coupled with location data taken from smartphones and vehicles, Beijing will increasingly be able to monitor the movements and behaviour of its citizens in unprecedented detail (Leibold, 2020). Gravette (2022) opines that these efforts will then merge with a vast database of information on every citizen, a ‘police cloud’ that aims to encompass criminal records, medical records, travel bookings, online purchases and even social media comments – and link all this information to every citizen's identity card and face. The national watchlist of would-be criminals and potential political agitators is already comprised of between 20,000,000 and 30,000,000 people (Vieweg, 2021).

China's vision for a real-time, nationwide surveillance network requires more than just ubiquitous video streaming and sensor data. According to Hung (2022), this Chinese vison also needs to leverage artificial intelligence to identify and track individuals across the network. As a result, Chinese companies, such as Hikvision (the world's largest manufacturer of surveillance equipment), Sensetime, Yitu and Megvii, have moved aggressively to meet this demand. These companies received over US$2,000,000,000 in government-initiated investment in 2018 (Vieweg, 2021). Thus to the eyes of the masses are added the brains of the country's fast-growing technology industry.

Scholars such as Gravette (2022) and Jia and Fanxu (2014) suggest that to evaluate just how effective China's novel model of digital authoritarianism could be, one has to look no further than China's far-flung western province of Xinjiang. It is an area in which individual freedom, liberty and security is absent, replaced by a comprehensive state surveillance system that aims for near total control. Xinjiang has become a window into the possible dystopian future of ubiquitous surveillance technology, wielded by states like China, states that have both the capital and political will to monitor – and repress – minority groups (Hicks, 2022). The Xinjiang Uyghur Autonomous Region is home to the Turkic Muslim ethnic minority Uyghur population of 11,000,000 people. In a country with an ethnic majority Han population, the central government in Beijing has long treated

Xinjiang as a 'frontier' in which the Uyghurs require pacification and assimilation. Accrding to Inkster (2021), the Chinese Communist Party has subjected the entire Uyghur population in Xinjiang to arbitrary arrest, draconian surveillance and systemic discrimination. One of the instances in which the massive surveillance capabilities of the Chinese state were seen during the 2014 Strike Hard Campaign Against Violent Terrorism. This Strike Hard campaign is unprecedented, not simply for its sheer scale in imposing social control, but also for its novel use and deployment of technology (Polyakova et al., 2019).

Concerns around the use of Chinese surveillance technologies in Africa center around the Chinese treatment of the Uyghur Muslims in what have been depicted as 'concentration camps' (Janus, 2021). Human Rights Watch has documented the Xinjiang authorities' collection of biometrics, including DNA samples, fingerprints, iris scans and blood types of all residents between the ages of 12 and 65. These biometric data, as well as voice samples, are collected as part of the passport application process. DNA and blood samples are collected by stealth, through a free, but obligatory, public health programme called 'Physicals for All' (Janus, 2021). Marvinet al., (2022) notes that residents of Xinjiang have absolutely no ability to challenge the collection, use, distribution or retention of their data. are also frequently forced to install spyware on their smartphones through which the government can track all of their online activity, identify the people they have called and record social media use. Wi-fi sniffers – probes that gather the unique addresses of devices such as laptops and smart phones – secretly collect data from all networked devices within range, and allow the government to covertly read users' e-mails (Gravette, 2022).

Most notably, the Human Rights Watch has described the Strike Hard Campaign in Xinjiang as arguably the world's largest open-air digital prison and an early glimpse of what digital authoritarianism might have in store (Woodhams, 2020). In its report *'Eradicating Ideological Viruses: China's Campaign of Repression Against Xinjiang's Muslims'*, it found human rights violations 'of a scope and scale not seen in China since the 1966–1976 Cultural Revolution' (Drollette Jr, 2022). The literature shows that not only is the regime of Xi Jinping persecuting millions of people based on their ethnicity and religion, but it is also developing tools of high-tech repression that could be used by dictatorships around the world and especially in Africa (Wang et al., 2023). Kara (2019) notes that this 'Orwellian model of repression' is likely to become the norm in China, and to be exported to like-minded totalitarian regimes elsewhere, unless the Xi regime encounters significant resistance.

Although China's presence in Africa has been growing steadily for 20 years, it started escalating drastically in 2013 following President Xi Jinping's unveiling of the Belt and Road Initiative (BRI). The BRI is a trillion dollar soft-power international development strategy to extend Beijing's influence in host countries through bilateral loans and infrastructure projects (Greitens, 2020). Most countries on the African continent have enthusiastically embraced the BRI. According to Dall'Agnola (2024), China has emerged as the largest source of financing for infrastructure projects in Africa and evidence of its influence is on display everywhere on the continent. China is also sponsoring thousands of the next generation of African leaders, bureaucrats, students and entrepreneurs to undergo training and education in China. China hosts tens of thousands of African university and postgraduate students every year, and the Chinese government offers thousands of scholarships to African students annually (Jili, 2022). The Hanban (the Chinese Language Council) has also founded 59 Confucius Institutes in Africa to propagate Chinese language and culture.

The BRI includes a major emphasis on information technology (Lokanathan, 2020). In Africa, China is unrivalled on the technological front. Lokanathan (2020) notes that large swaths of the continent have fundamentally come to rely on Chinese companies for their telecommunications and digital services. China Telecom plans to lay a 150,000km fibre optic network covering 48 African nations (Lokanathan, 2020). Transsion Holdings, a Shenzhen-based company, has overtaken Samsung to become the leading smartphone provider in Africa. Huawei, the Chinese telecommunications giant, has built 70 per cent of the 4G networks and most of the 2G and 3G networks on the continent, vastly outpacing its European rivals (Agbebi, 2022). The Kenyan government has also appointed Huawei as principal advisor on its 'master plan' for information and communication technologies. The Chinese telecommunications conglomerate, ZTE, provides the Ethiopian government with infrastructure to enable it to monitor and surveil communications by opposition activists and journalists (Jili, 2022). Another Chinese company, H3C, has won the contract to construct the Nigerian airport's new telecommunications network. Hikvision has established an office in Johannesburg and

through a local video surveillance provider has rolled out 15,000 cameras throughout the Johannesburg metropolitan area in 2019 (Tambo et al., 2019). Zimbabwe's state owned telecommunications companies such as NetOne have running contracts with Huawei.

Methodological approach

This study employed a desk research approach to examine the coloniality of Chinese surveillance technologies in Africa. This research analysed existing secondary data sources which included government and Non-Governmental Organizations reports, legal documents and media publications. The desk research also perused relevant academic literature relevant to the study. Databases such as Google Scholar, JSTOR, and ResearchGate were utilised to access peer-reviewed journal articles, book chapters, and conference proceedings. This process aimed to gather insights from existing scholarly work, identify gaps in the literature, and develop a comprehensive understanding of the theoretical and empirical foundations of the topic. Additionally, policy papers on the corporations between African states and the Chinese Republic in areas around security and economic cooperation were also perused. The review of these sources provided valuable insights into the frameworks and policy implications surrounding the transfer of Chinese surveillance technologies to African contexts and the resultant implications of such. Data triangulation, involving cross-verification of information from multiple sources, was conducted to enhance the validity of the findings. Due care was taken to ensure the accuracy and objectivity of the data analysis, avoiding biases and misrepresentations.

FINDINGS AND DISCUSSION

Neo-colonial dynamics

The proliferation of Chinese surveillance technologies in African nations have been seen as a contemporary form of colonialism, where power dynamics and exploitation mirror historical colonial practices. The Chinese surveillance technologies expansion in Africa exemplifies neo-colonial dynamics, particularly through economic influence and political relationships that reshape local governance and societal structures. Chinese investments in surveillance infrastructure, such as the deployment of extensive CCTV systems in countries like Ethiopia and Kenya, illustrate how these technologies often come with financial agreements that prioritize Chinese firms and labor over local alternatives. For example, Woodhams (2020) reported that the Ethiopian government has increasingly relied on Chinese technology to bolster its surveillance capabilities which has led to concerns about human rights violations and the erosion of civil liberties. In *"Total Liberation: The Power and Promise of Animal Rights and the Radical Green Movement"*, Pellow (2014) argue that such investments create economic dependencies reminiscent of colonial practices. In this scenario, African nations become beholden to foreign capital and technological expertise from the Chinese People's Republic. This dependency is compounded by the "debt trap" diplomacy often associated with Chinese investments, as seen in Zambia, where the government has struggled to repay loans tied to infrastructure projects (Mutai et al., 2024). These circumstances undoubtedly hinder Africa's economic autonomy and cedes control over critical national assets to powerful Chinese entities.

Furthermore, the collaboration between China and African governments in areas of technology has significantly altered governance structures. In the African Report of 20 March 2023, the Zimbabwean government's use of Chinese surveillance technologies to monitor and suppress opposition highlights the implications for democratic governance and human rights. Benner et al., (2018) demonstrated how these partnerships can lead to increased authoritarianism. State surveillance mutates into a tool for repression rather than public safety. This trend is evident in the way Chinese technologies enable governments to maintain tight control over dissent, often at the expense of citizens' rights (Gagliardone, 2022). in line with that, the resistance against these technologies is gaining momentum, particularly among youth and activists who leverage social media platforms to challenge the implications of such surveillance systems. In South Africa, significant pushback against facial recognition technologies has emerged. Activists in South Africa have argued that these systems exacerbate issues of privacy violations and racial profiling, particularly against marginalized communities (The Sowetan, March 2022). This resistance not only reflects a growing awareness of the

implications of surveillance but also underscores a broader cultural struggle against the erasure of local identity and agency that can accompany the imposition of foreign technologies.

Economic interests and investments

Many nation states in Africa have argued that they are embracing Chinese technologies due to the many economic possibilities they offer (Feldstein, 2020). One typical example is the Police in Uganda, where a huge purchase of Chinese cameras was completed in order to curb crime which was said to be an anathema to economic development in the business hubs of Kampala and other major cities (Jili, 2022). In 2021, the Zimbabwean President Emmerson Mnangangwa boasted of the economic benefits that would accrue from the Chinese built National Data Centre in Zimbabwe. This theme may focus on the economic motivations behind the partnership between African nations and China, including investments in infrastructure and technology that prioritize profit over ethical considerations. The interplay between economic interests and investments in the context of Chinese surveillance technologies in Africa reveals a complex landscape characterized by neo-colonial dynamics (Sheombar and Skelton, 2023).

Chinese firms have rapidly expanded their presence across the continent, positioning themselves as critical partners in infrastructural development. For instance, the establishment of extensive surveillance systems in countries like Ethiopia and Kenya is frequently accompanied by significant financial investments and technology transfers, framed as mutually beneficial partnerships. However, Bräutigam (2011) in her book *"The Dragon's Gift: The Real Story of China in Africa"* argue that these arrangements often prioritize Chinese economic interests, overshadowing local development needs and aspirations. In Ethiopia, the deployment of surveillance technologies has been linked to Chinese state-owned enterprises, raising concerns about the sustainability of such investments and their long-term implications for local economies (Jili, 2022). Critics point out that while these technologies may enhance security, they also perpetuate a cycle of dependency that stifles local innovation and economic autonomy, reflecting a modern iteration of the exploitative practices seen during colonial times. Munoriyarwa and Chiumbu (2022) aver that this dynamic not only reinforces economic subservience but also erodes local capacities to engage with and develop alternative technological solutions.

Moreover, the economic interests underlying these investments often manifest in broader geopolitical strategies that seek to secure resources and influence in Africa. China's BRI exemplifies this approach, as it establishes infrastructure and connectivity across the African continent (Burnay, 2019). It is in this initiative that surveillance technologies are being a key component. For example, in Zambia, the government has embraced Chinese surveillance systems to monitor urban areas, ostensibly to combat crime. However, Blaubach (2021) assert that this has raised alarms about the implications for civil liberties and the potential for state overreach. Taylor (2009) noted that such investments create a dual dependency where African nations rely on Chinese technology and financing, while China secures access to vital resources and strategic alliances. Brunner and DeLuca (2019) are of the view that this pattern often leaves African countries vulnerable to exploitation, as the economic benefits of such partnerships are frequently unevenly distributed, favoring Chinese firms and investors. As a result, the economic interests at play in the realm of surveillance technologies underscore the enduring legacy of colonial relationships, wherein external powers exert significant influence over local economic and political landscapes.

Furthermore, the ramifications of these investments extend beyond immediate economic benefits, impacting social and cultural dimensions within African societies. The influx of Chinese surveillance technologies often comes with a cultural imperialism that imposes foreign norms and practices, which can undermine local governance and social structures (Feldstein, 2021). For instance, in South Africa, the government's interest in adopting Chinese surveillance systems has sparked debates about privacy rights and the potential erosion of democratic freedoms. Activists argue that these technologies may not only facilitate state control but also contribute to a culture of surveillance that normalizes intrusive monitoring of citizens (Tai, 2015). This cultural shift raises critical questions about agency and the power dynamics between citizens and the state, echoing the socio-political hierarchies established during colonial rule. The embrace of foreign technologies, particularly those with surveillance capabilities, thus reflects a deeper struggle over identity, autonomy, and governance in contemporary African societies, emphasizing that economic interests are intricately tied to broader issues of power and control in the post-colonial context.

Resistance and agency

Most narratives on the transfer of Chinese surveillance technologies have placed emphasis on the uncontrollable and unstoppable power of Chinese influence in African states. Little attention has been given to agency and local responses to the imposition of Chinese surveillance technologies especially in the context of repressive and autocratic regimes (Woodhams, 2020). The role of non-state actors, and civil society groups has largely been muted in literature. This takes away the agency and resistance that has been going on in some African states to the integration of such technologies. Tufekci (2017) is of the view that the increase in corporation between African states and China on areas of security has led to an emergency of grassroots movements and some form of political strategies that is aimed at rescuing the agency and assert control over the use of such technology in African contexts.

The most prevalent argument with regards to the expansion of Chinese influence on African authoritarian regimes has been that the methods it used to discipline its media have also been adopted, hook-line and sicker in such African states (Hicks, 2022). This has led to the idea that these Chinese surveillance technologies have led to the shrinking of civil liberties and civil space. The African Report Magazine of 11 July 2024 seem to give credence to the idea that Chinese surveillance technologies enable repressive regimes in Africa to spy on its citizens. The case is emboldened by the Edward Snowden case, where the National Security Agency illegally collecting data of millions of citizens for spying reasons. According to Khalil (2020), the same trend has been observed in Africa, where autocratic states arrest dissenting voices on information that is gathered using surveillance on their social media handles. For instance, Zimbabwe's top journalist Hopewell Chin'ono was arrested on 8 January 2021 for ''communicating falsehoods'' on the Twitter platform, now X (The Guardian UK, January 2021). Elsewhere, Job Sikhala, a prominent opposition figure in Zimbabwe was also arrested and convicted for publishing information prejudicial to the state' (The Herald Zimbabwe, 8 February 2024). Although his defence vehemently protested that the account was not his own, the state highlighted that it had a strong case against him. Irrespective of the evidence of these case and how they were used to suppress online activisms by the Zimbabwean government, they have been efforts by online communities to resist this encroachment by the state. For instance, the civil society in Uganda has attempted may inductions against the police for using the technology acquired from China such as surveillance cameras to spy on encrypted communications by senior opposition figures in the country such as Bobi Wine. Actors within the civil society have called for constitutional safeguards. The call for institutional protection mechanisms have been growing loud in countries such as Ghana and Nigeria so as to protect citizens from political surveillance and oppression (Dimitrov, 2024).

The several media reports from across Southern Africa and West Africa have highlighted the dynamics of resistance and agency in the context of Chinese surveillance technologies in Africa (Rothschild, 2024). These issues illustrate a profound struggle over power, identity, and autonomy amidst neo-colonial influences championed by imported Chinese surveillance technologies. As African nations increasingly adopt Chinese technologies purportedly for surveillance and security where local communities are not merely passive recipients but are actively engaging in resistance against what they perceive as intrusive and oppressive measures (Blaubach, 2021). In countries like South Africa, activists have mobilized through social media platforms to challenge the implementation of facial recognition systems, arguing that these technologies disproportionately target marginalized groups and violate fundamental rights to privacy and freedom of expression. Scholars such as Dever and Dever (2020) emphasize that such grassroots movements reflect an assertion of agency, wherein citizens actively negotiate their relationship with the state and external powers (Dimitrov, 2024). This form of resistance underscores the importance of local narratives and the need for inclusive dialogues about technology deployment, emphasizing that communities should have a say in the surveillance measures that affect their lives.

Moreover, Grinberg (2017) opines that this resistance is often rooted in a broader awareness of historical injustices and the ongoing implications of neo-colonialism. In Zimbabwe, the civil society organizations have been vocal against the use of Chinese surveillance technologies to monitor political dissent. Activists argue that these systems not only facilitate government repression but also echo the historical patterns of control reminiscent of colonial rule (Reddy, 2021). Scholars like Yuen (2015) and Reddy (2021) have pointed out that such resistance movements often draw strength from collective memory and shared experiences of oppression.

This collective resistance enables communities to articulate a vision for a more equitable future that prioritizes human rights over state control. This collective agency is also critical in shaping public discourse around surveillance and this pushes for accountability and transparency from both local governments and foreign investors (Dever et al., 2020). The growth of these movements grow challenge the prevailing narratives that frame surveillance technologies as necessary for security and in the process highlighting the risks of increased authoritarianism and social fragmentation.

The emergence of resistance movements to the entrenchment of Chinese surveillance technologies in Africa is also influenced by the evolving landscape of technology and communication. The proliferation of digital platforms has empowered activists and ordinary citizens alike to organize, share information, and mobilize against surveillance practices (Lin, 2024). For instance, campaigns like #NoToSurveillance in various African countries have gained traction. This has resultantly created a digital space for dialogues about privacy and state overreach. This digital activism raises awareness about the implications of surveillance technologies and fosters a sense of solidarity among diverse groups facing similar challenges (Oxford Analytica, 2022). Tufekci (2017) in the book *"Twitter and Tear Gas: The Power and Fragility of Networked Protest"* argue that the ability to connect and coordinate through social media platforms enhances the capacity of local movements to resist external control. This evolution in resistance signifies a shift towards a more informed and engaged citizenry that is increasingly unwilling to accept external impositions without scrutiny. This resistance also highlights the vital role of citizen engagement in shaping the future of governance and societal norms in Africa and ultimately, the deployment and use of surveillance technologies in the future.

Geopolitical dynamics

The geopolitical dynamics surrounding the adoption of Chinese surveillance technologies in Africa are complex and multifaceted. According to Gravett (2023), these dynamics reflect a blend of local agency, international relations, and the strategic interests of both African states and China. As African nations increasingly procure surveillance tools from China, they navigate a landscape shaped by historical legacies of colonialism and contemporary power relations. For instance, Kenya's collaboration with Chinese firms to implement advanced surveillance systems such as the installation of facial recognition technology in urban areas illustrates how local governments seek to enhance public security while simultaneously aligning with China's broader geopolitical ambitions in the region (Lin, 2024). This partnership not only underscores Kenya's desire to modernize its security infrastructure but also highlights China's strategic investment in establishing a foothold in African markets, thereby expanding its influence across the continent (Jili, 2022; Feldstein, 2019). The implications of these technologies extend beyond mere security enhancements; they also reflect a shift in the balance of power within the geopolitical landscape of Africa, as countries increasingly rely on Chinese technology to address local governance challenges (Hoffman, 2019; Ahrens, 2013).

Moreover, the implications of these surveillance technologies extend beyond mere security enhancements; they also reflect a shift in the balance of power within the geopolitical landscape of Africa. Countries like Uganda have embraced Chinese surveillance systems to bolster state control, often at the expense of civil liberties. The Ugandan government's use of Chinese technology to monitor political dissent and suppress opposition movements exemplifies how these tools can reinforce authoritarian governance under the guise of maintaining public order (Jili, 2022; Feldstein, 2019). This trend raises critical questions about the long-term consequences of such partnerships, as African states may find themselves increasingly beholden to Chinese technological and financial support, potentially compromising their sovereignty and democratic processes (Ahrens, 2013). The interplay between local governance needs and external influences from China creates a precarious situation where the benefits of enhanced security may come with significant costs to individual freedoms and democratic norms, as evidenced by the growing concerns over human rights violations associated with the deployment of these technologies (Woodhams, 2020).

The broader geopolitical implications of China's surveillance technology in Africa also resonate within the context of U.S.-China competition. As the United States and its allies express concerns over China's growing influence in Africa, particularly regarding human rights and governance issues, there is a pressing need for a more nuanced understanding of African agency in these dynamics (Hoffman, 2019; Ahrens, 2013). African nations are not merely passive recipients of Chinese technology; they actively engage in shaping their

relationships with external powers based on their national interests and security needs. For example, South Africa's cautious approach to adopting Chinese surveillance technologies reflects a desire to balance its partnerships with both China and Western nations, highlighting the complexities of navigating geopolitical pressures while striving for national autonomy (Jili, 2022; Feldstein, 2019). This evolving landscape necessitates a reevaluation of how international actors engage with African states, emphasizing the importance of supporting local governance frameworks that prioritize human rights and democratic values amidst the proliferation of surveillance technologies (Hoffman, 2019; Ahrens, 2013).

CONCLUSIONS AND RECOMMENDATIONS

The findings regarding the proliferation of Chinese surveillance technologies in Africa reveal significant neo-colonial dynamics that warrant careful consideration and action. The expansion of these technologies often mirrors historical colonial practices, where African nations become economically and politically dependent on foreign powers, particularly China. This dependency is exacerbated through financial agreements that favor Chinese firms and labor, as observed in Ethiopia and Kenya, where extensive surveillance systems have been deployed under the guise of enhancing security (Hoffman, 2019; Jili, 2022). Such investments not only raise concerns about human rights violations but also threaten the autonomy of African nations, as they become beholden to Chinese capital and technological expertise, echoing the exploitative relationships of the colonial era (Pellow, 2020). The implications of this dependency are profound; local governance structures are reshaped in ways that prioritize external interests over the needs of citizens, leading to a loss of agency and control over national security measures (Ahrens, 2013).

In light of these findings, it is crucial for African governments to prioritize the establishment of robust regulatory frameworks that govern the deployment and use of surveillance technologies. This includes ensuring that local communities are actively involved in discussions about technology adoption, thereby safeguarding their rights and interests (Brunner et al., 2019). Resistance movements emerging across the continent, particularly among youth and civil society groups, highlight the importance of agency in confronting the imposition of foreign technologies. Activists in South Africa have successfully challenged facial recognition systems, emphasizing the need for privacy rights and the protection of marginalized communities (The Sowetan, 2022; Bräutigam, 2020). Furthermore, these movements serve as a catalyst for broader societal engagement, encouraging citizens to question the motivations behind surveillance initiatives and advocate for transparency (Pellow, 2020). By fostering an environment that encourages public discourse and civic engagement, African nations can reclaim agency over their technological landscapes and resist neo-colonial influences that threaten democratic processes and civil liberties (Dimitrov, 2024).

Moreover, it is essential for African states to engage in strategic partnerships that prioritize local development needs and aspirations over foreign economic interests. The current trend of embracing Chinese surveillance technologies often overlooks ethical considerations and the long-term implications for governance and civil liberties (Bräutigam, 2020). Scholars like Bräutigam (2020) argue that these partnerships should be reframed to ensure that they contribute to sustainable development and empower local economies rather than perpetuate cycles of dependency (Ahrens, 2013). This could involve negotiating terms that favor local firms and labor, thus cultivating a more equitable technological ecosystem that aligns with socio-economic goals (Jili, 2022). Additionally, African governments should explore alternative partnerships with technology providers that adhere to principles of ethical governance and respect for human rights (Feldstein, 2019). Such a proactive approach can lead to innovations that reflect local contexts and foster resilience against external pressures.

The geopolitical dynamics surrounding the adoption of Chinese surveillance technologies necessitate a reevaluation of international relations in Africa. As African nations navigate their relationships with external powers, it is vital to emphasize the importance of human rights and democratic values (Woodhams, 2020). The growing concerns over human rights violations associated with these technologies call for a collaborative approach among African states, international actors, and civil society to promote accountability and transparency in governance (Feldstein, 2019). The historical context of colonial exploitation adds urgency to this discourse; African nations must not only protect their sovereignty but also assert their right to shape their technological futures (Hoffman, 2019; Bräutigam, 2020). By fostering a collective commitment to uphold democratic principles, African nations can mitigate the risks associated with foreign surveillance technologies

and assert their sovereignty in the face of neo-colonial pressures (Rothschild, 2024). This multidimensional strategy will not only enhance national security but also promote a model of development that prioritizes citizen empowerment and social justice.

REFERENCES

1. A. Polyakova and C. Meserole, 'Policy Brief: Exporting digital authoritarianism: the Russian and Chinese Models', Brookings Institution (August 2019).
2. Agbebi, M. (2022). China's Digital Silk Road and Africa's technological future.
3. Ahrens, N. (2013) China's Competitiveness Myth, Reality, and Lessons for the United States and Japan. Center for Strategic and International Studies. Available at: https://csis-website-prod.s3.amazonaws.com/s3fspublic/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf (Accessed: 20 January 2025).
4. Benner, T., Gaspers, J., Ohlberg, M., Poggetti, L., & Shi-Kupfer, K. (2018). Authoritarian advance: responding to China's growing political influence in Europe.
5. Blaubach, T. (2021). Chinese technology in the Middle East: A threat to sovereignty or an economic opportunity.
6. Brautigam, D. (2011). The dragon's gift: the real story of China in Africa. oUP oxford.
7. Bräutigam, D. (2020) *The Dragon's Gift: The Real Story of China in Africa*. Oxford University Press.
8. Brunner, E. A., & DeLuca, K. M. (2019). Creative confrontations: Exploring activism, surveillance, and censorship in China and the United States. IAFOR Journal of Psychology & the Behavioral Sciences, 5(si), 75-88.
9. Burnay, M. (2019). Privacy and surveillance in a digital era: transnational implications of China's surveillance state. EUCROSS.
10. Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. Journal of Cyber Policy, 3(3), 306-326.
11. Dall'Agnola, J. (2024). Keeping Watch Along the Digital Silk Road. Seeing China's Belt and Road, 164.
12. Dever, J., & Dever, J. (2020). Information Age Imperialism: China,'Race,'and Neo-Colonialism in Africa and Latin America. U. Miami Inter-Am. L. Rev., 52, 1.
13. Dimitrov, M. K. (2024). Exporting Chinese Digital Authoritarianism. In Routledge Handbook on Global China (pp. 170-181). Routledge.
14. Doshi, R., de La Bruyere, E., Picarsic, N., & Ferguson, J. (2021). China as a cyber great power: Beijing's two voices in telecommunications.
15. Drollette Jr, D. (2022). The high-tech surveillance state is not restricted to China: Interview with Maya Wang of Human Rights Watch. Bulletin of the Atomic Scientists, 78(5), 239-242.
16. Feldstein, S. (2019) The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 (Accessed: 20 January 2025).
17. Feldstein, S. (2020, May). Testimony before the US-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa May 8, 2020.
18. Feldstein, S. (2021). The rise of digital repression: How technology is reshaping power, politics, and resistance. Oxford University Press.
19. Gagliardone, I. (2022). Impact of Chinese Tech Provision on Civil Liberties in Africa. South African Institute of International Affairs.
20. Germanò, M. A., Liu, A., Skebba, J., & Jili, B. (2023). Digital surveillance trends and Chinese influence in light of the COVID-19 pandemic. Asian Journal of Comparative Law, 18(1), 91-115.
21. Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. African Human Rights Law Journal, 20(1), 125-146.
22. Gravett, W. H. (2023). Digital coloniser? China and artificial intelligence in Africa. In Survival December 2020–January 2021: A World After Trump (pp. 153-177). Routledge.
23. Greitens, S. C. (2020). Dealing with demand for China's global surveillance exports. Brookings Institution Global China Report.

24. Grinberg, D. (2017). Chilling developments: digital access, surveillance, and the authoritarian dilemma in Ethiopia. Surveillance & Society, 15(3/4), 432-438.
25. Hicks, J. (2022). Export of Digital Surveillance Technologies from China to Developing Countries.
26. Hoffman, S. (2019) China's Tech-Enhanced Authoritarianism. House Permanent Select Committee on Intelligence. Available at: https://intelligence.house.gov/uploadedfiles/2019-09-20_china_tech-enhanced_authoritarianism.pdf (Accessed: 20 January 2025).
27. Hung, H. T. B. (2022). Keep your eyes on China's metaverse: Another tool for maintaining its national security. The Journal of Intelligence, Conflict, and Warfare, 5(2), 1-31.
28. Inkster, N. (2018). China's cyber power. Routledge.
29. Inkster, N. (2021). The great decoupling: China, America and the struggle for technological supremacy. Hurst Publishers.
30. Janus, D. (2021). Smart cities in China: sustainable or surveyed. Sprawy Międzynarodowe, 74(1), 153-174.
31. Jia, L., & Fanxu, Z. (2014). Microblogging and grassroots surveillance in China. China: An International Journal, 12(3), 55-71.
32. Jili, B. (2022) What is driving the adoption of Chinese surveillance technology in Africa? Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/ (Accessed: 20 January 2025).
33. Jili, B. (2022). The Spread of Chinese Surveillance Tools in Africa: A Focus on Ethiopia and Kenya. In Africa–Europe Cooperation and Digital Transformation (pp. 32-49). Routledge.
34. Kara, H. (2019). Human Rights in China In The Xi Jinping Era: From The Perspective of Human Rights Watch and Amnesty International. Doğu Asya Araştırmaları Dergisi, 2(1), 66-96.
35. Khalil, L. (2020). Digital authoritarianism, China and C0VID.
36. Leibold, J. (2020). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. Journal of contemporary China, 29(121), 46-60.
37. Lin, B. (2024). Beyond authoritarianism and liberal democracy: Understanding China's artificial intelligence impact in Africa. Information, Communication & Society, 27(6), 1126-1141.
38. Lokanathan, V. (2020). China's belt and road initiative: Implications in Africa. Observer Research Foundation, 27.
39. Marvin, S., While, A., Chen, B., & Kovacic, M. (2022). Urban AI in China: Social control or hyper-capitalist development in the post-smart city?. Frontiers in Sustainable Cities, 4, 1030318.
40. Munoriyarwa, A., & Chiumbu, S. H. (2022). Powers, Interests and Actors 1: The Influence of China in Africa's Digital Surveillance Practices. In Digital Dissidence and Social Media Censorship in Africa (pp. 209-229). Routledge.
41. Mutai, N. C., Cuong, N. M., Dervishaj, V., Kiarie, J. W., Misango, P., Ibeh, L., ... & Lallmahamood, M. (2024). Examining the sustainability of African debt owed to China in the context of debt-trap diplomacy. Scientific African, 24, e02164.
42. Naguib Pellow, D. (2014). Total Liberation: The Power and Promise of Animal Rights and the Radical Earth Movement. Social Policy, 44(4).
43. Oxford Analytica. (2022). Digital authoritarianism in Africa is evolving. Emerald Expert Briefings, (oxan-db).
44. Pellow, D. (2020) The Politics of Surveillance in Africa: The Case of China's Digital Expansion. *African Studies Review*, 63(2), pp. 1-20.
45. Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models. Policy brief, democracy and disorder series, 1-22.
46. Reddy, R. K. (2021). Mapping China's presence in Africa's digital economy. Institute of Peace and Conflict Studies, Delhi, 15.
47. Rothschild, V. (2024). Protest and repression in China's digital surveillance state. Journal of Information Technology & Politics, 1-16.
48. Sheombar, A., & Skelton, S. K. (2023, December). Follow the surveillance: A breadcrumb trail of surveillance technology exports to Africa. In IFIP Joint Working Conference on the Future of Digital Work: The Challenge of Inequality (pp. 241-261). Cham: Springer Nature Switzerland.
49. Sun, Y., & Yan, W. (2020). The power of data from the Global South: environmental civic tech and data activism in China. International Journal of Communication, 14, 19.

50. Tai, Z. (2015). Networked resistance: Digital populism, online activism, and mass dissent in China. Popular Communication, 13(2), 120-131.
51. Tambo, E., Khayeka-Wandabwa, C., Muchiri, G. W., Liu, Y. N., Tang, S., & Zhou, X. N. (2019). China's Belt and Road Initiative: Incorporating public health measures toward global economic growth and shared prosperity. Global Health Journal, 3(2), 46-49.
52. Taylor, I. (2009). *China's new role in Africa*. Boulder, CO: Lynne Rienner Publishers.
53. Tufekci, Z. (2017). Twitter and tear gas: The power and fragility of networked protest. Yale University Press.
54. Velghe, P. (2019). “Reading China”. The Internet of Things, Surveillance, and Social Management in the PRC. China Perspectives, 2019(2019-1), 85-89.
55. Vieweg, S. H. (2021). AI and the Ethical Challenge. In AI for the Good: Artificial Intelligence and Ethics (pp. 143-157). Cham: Springer International Publishing.
56. Wang, M., Kaltheuner, F., & Klasing, A. (2023). The future of technology: Lessons from China. Bulletin of the Atomic Scientists, 79(3), 170-173.
57. Woodhams, S. (2020). China, Africa, and the private surveillance industry. Geo. J. Int'l Aff., 21, 158.
58. Woodhams, S. (2020). China, Africa, and the private surveillance industry. Geo. J. Int'l Aff., 21, 158.
59. Yuen, S. (2015). Becoming a cyber power. China’s cybersecurity upgrade and its consequences. China Perspectives, 2015(2015/2), 53-58.