The Interest Behind Cyber-Attacks Targeting Africa and Attributed to the Region: Analysing Chinese Influence Behind Cyber-Operations in Africa[1]

Noémi Csunyó[2]

Abstract:

Over the past decade, the global importance of cybersecurity has steadily increased as states, companies and societies have become increasingly reliant on digital infrastructures. In parallel, Africa is undergoing a digital transformation, but this rapid growth is often not matched by adequate cybersecurity capabilities, making many states particularly vulnerable to cyber threats. In this rapidly changing environment, China's growing technological presence and expansion in Africa are noteworthy, not only in terms of economic and infrastructural support, but also in the form of a new type of digital influence. The primary objective of the research is to explore the types of technological and financial support China is providing to African countries in the digital sector, the extent to which and how this support is contributing to the development of African states' cyber capabilities. Within this context, the study also analyses the types and characteristics of cyber operations in the region, the possible underlying motivations, and the types of actors (state-sponsored actors, cybercriminals or hacktivists) and their presence behind the attacks. The research will also seek to assess how China affects the digital sovereignty of African countries and its impact on security policy in the region.

Keywords:

China; Africa; influence; cyber; digitalisation.

[1] DOI: 10.12700/jceeas.2025.5.4.423

[2] Researcher and PhD Student at the Institute of World Economy and International Relations, University of Debrecen, Hungary; ORCID: 0000-0002-4864-7116; csunyo.noemi97@mailbox.unideb.hu.

1. Introduction

In recent decades, China has emerged as a dominant player in Africa, extending its influence beyond economic activity to encompass the political and social spheres. It is Africa's largest creditor, accounting for approximately 17% of the sub-Saharan region's external public debt (USD 134 billion) as of 2023 (Munyati, 2024).

Furthermore, foreign direct investment (FDI) has increased significantly in recent years. According to the latest United Nations Conference on Trade and Development (UNCTAD) report, foreign direct investment (FDI) inflows to the African continent increased by 75% in 2024 compared to the previous year, reaching $97 billion (representing 6% of global FDI, compared to 4% the previous year) (UNCTAD, 2025).

Conversely, the United States is also allocating considerable financial resources to African territories, as illustrated in Figure 1, in comparison with Chinese FDI.

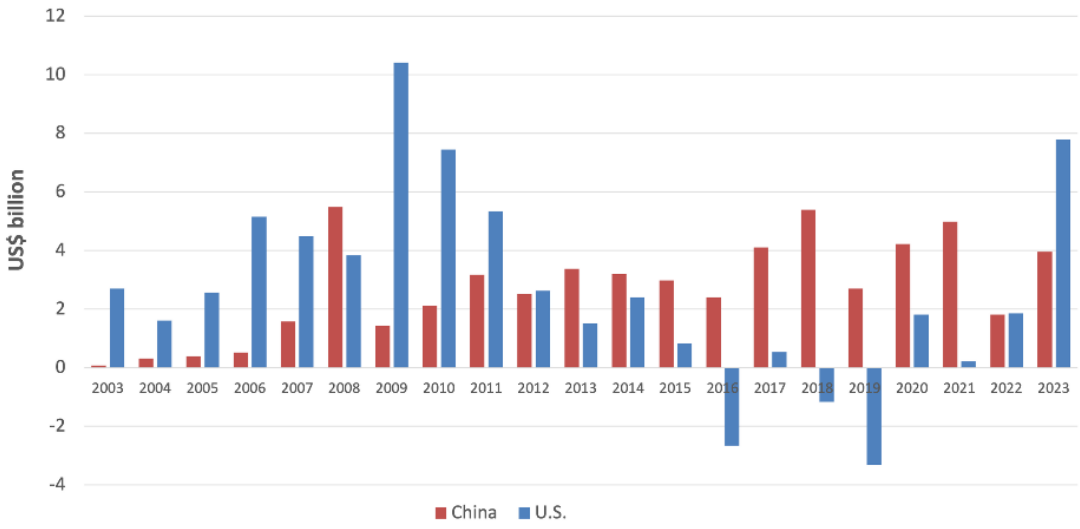

Figure 1: Chinese and US FDI to Africa (flow)
Source: China Africa Research Initiative (2025)

Over the period 2010-2023, Chinese FDI ranged between 4% and 11%, showing a stable presence, while the US investment demonstrated a more cyclical pattern, characterised by frequent capital withdrawals. China's strong presence shows that its plans are long-term, while the US presence is rather short-term and exposed to market fluctuations.

FDI remains dominated by European and American sources, but China is now firmly in third place (USD 42 billion in 2024), and its investments are becoming increasingly diversified.[3] One-third of projects within China's Belt and Road Initiative (BRI) are already focused on social infrastructure and renewable energy (UNCTAD, 2025).

Note: Although statistics show that Africa attracts around 7% of Chinese FDI, and up to 15% by value, these figures are often misleading. They often include projects that have

[3] The main recipients of Chinese FDI are Niger, South Africa, Angola, Morocco and the Republic of Congo, while US investments are mainly directed towards Egypt, South Africa and Nigeria (China Africa Research Initiative, 2025).

never been implemented, or in many cases do not represent actual FDI but rather loans. Furthermore, most Chinese investments are not export-oriented, focusing mainly on mining, manufacturing, and light industry, producing for the local market. This means that the real economic impact of Chinese-African investments is more modest than official numbers suggest, and Africa's economic transformation is progressing more slowly than expected (Paterson, 2024).

The African continent is not only the target of competition between major powers but is also increasingly becoming an active scene. Several major powers (including China, the US, Russia, the EU and Turkey) are attempting to increase their influence in Africa in various ways[4] (Gopaldas, 2022). African countries are particularly vulnerable due to the high import dependence of their technological infrastructure. The continent remains exposed to the technological decisions of major powers and to disruptions in global supply chains (Ayodele, 2022).

The Chinese presence is not only aimed at developing infrastructure, but also at building close political alliances that will help strengthen China's global position. These efforts are closely aligned with the African Union's Agenda 2063, particularly the objectives of the Programme for Infrastructure Development in Africa (PIDA) and the African Continental Free Trade Area (AfCFTA), which aim to establish a unified and interconnected African economy (Kluiver, 2025).

It is inaccurate to assert that African development is exclusively reliant on Chinese investment; however, it is evident that the growth in Chinese investment has played a substantial role in establishing the foundations for critical digital and physical infrastructure, including railways, ports, 5G networks, and data centres.

2. Materials and Methods

The current article focuses on how Chinese investment has contributed to the development of digital technology in Africa and how this development has improved the cyber capabilities of African countries. The aim is to analyse how the region's growing influence and digital maturity have made it more vulnerable to cyber-attacks and how these factors affect the region's security posture. This is conducted through the examination of the cyberattacks that have been observed in the region, encompassing their underlying motivations and the characteristics of the attackers. This analysis relies on qualitative methods, including document analysis and case studies, to provide a comprehensive understanding of the threats. The research provides insight into a relatively understudied but strategically significant aspect of Sino-African relations.

3. China's Digital Influence on the Continent

China's influence in Africa is no longer limited to economic and infrastructure investment (Nelson, 2024). In recent years, the nature of cooperation between China and Africa has evolved, with the strengthening of economic and trade relations being complemented by an increasing importance placed on security and technological ties (Krukowska, 2024).

Figure 2 shows the value of Chinese ICT and machine exports to African countries between 2015 and 2020.

[4] The US and Europe often use soft power, which takes the form of diplomacy, development aid and educational programmes (Gopaldas, 2022).

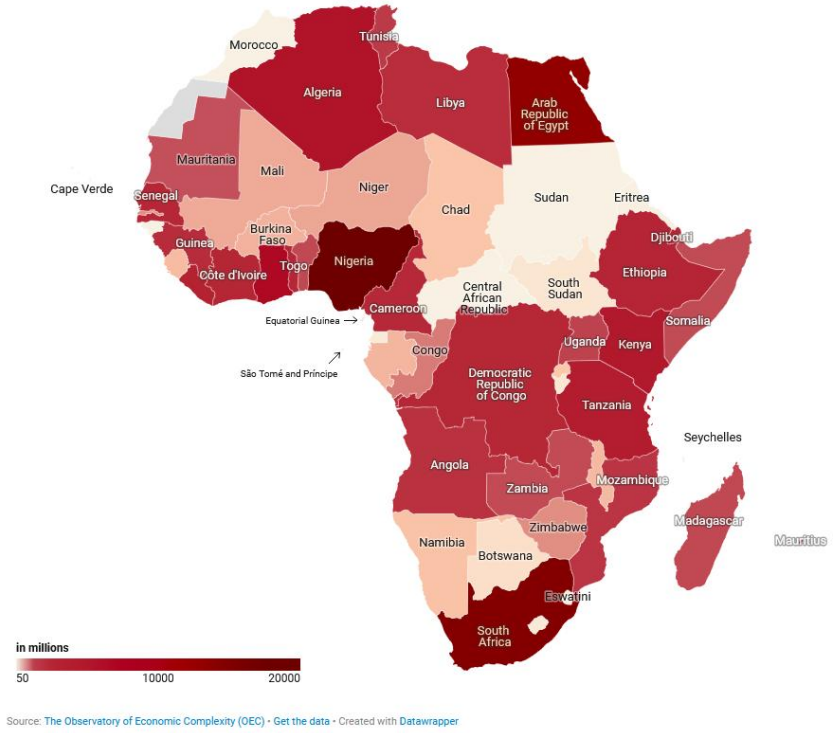

Figure 2: Value of Chinese ICT and machine exports to Africa between 2015 and 2020
Source: Good Governance Africa (2022)

Nigeria, South Africa, and Egypt stand out as the largest importers, each receiving exports worth up to $20 billion. This reflects their relatively larger economies, more developed ICT sectors, and strategic roles in regional trade. Significant import volumes are also concentrated in Algeria, Angola, Kenya, and Ethiopia, suggesting strong Chinese engagement in infrastructure and technology projects there. Central African countries such as Chad, South Sudan, and several smaller economies have much lower figures, likely due to smaller markets, weaker infrastructure, or political instability limiting large-scale trade. The data aligns with China's Belt and Road Initiative footprint in Africa, with high-value exports often going to countries where China is investing heavily in ports, telecommunications, energy grids, and urban infrastructure. Overall, the map highlights how China's ICT and machinery exports are concentrated in Africa's largest economies and strategic hubs, reinforcing both economic ties and long-term technological dependence in these regions.

In recent years, there has been an increasing emphasis on technological, digital and security cooperation, which has positioned China not only as a 'builder' but also as a key driver of digital development on the continent.[5] The concept of the Digital Silk Road has opened up new dimensions as part of the One Belt, One Road Initiative (BRI), where Chinese companies are exporting data centres, telecom networks, smart city solutions and complex IT infrastructure to Africa. The provision of technology solutions by Chinese companies is a major contributing factor to the modernisation of local firms, with cloud-based systems, online payment platforms and e-commerce (Huang and Pollio, 2023). The Digital Silk Road initiative has enabled China

[5] Between 2001 and 2021, China significantly expanded its technological footprint in Africa and has since become the continent's leading technology exporter (Rojo, 2023).

to assume a more prominent role in establishing standards for digital governance, privacy and cybersecurity, thereby exporting its own authoritarian model of internet governance[6] (Article 19, 2024). For African countries, Chinese technologies – due to their low cost, flexible financing, and quick access – often better suit development needs than Western sources, which tend to impose stricter conditions (Prakash, 2025). Chinese cooperation generally does not impose requirements regarding compliance with the rule of law or human rights standards (Gariba, 2022).

Comprehensive digital infrastructure is an attractive alternative for many countries on the continent (Prakash, 2025). The digital sector has become one of the fastest-growing areas of China's economic presence in Africa. At the 2024 FOCAC Summit, Beijing highlighted the importance of cooperation with African countries in cybersecurity, artificial intelligence (AI) and global digital governance rulemaking (Article 19, 2024). Furthermore, China has announced a commitment of RMB 350 billion (approximately USD 50 billion) to support digital development in Africa. The structure of the investment, whether in the form of an investment or a loan, remains to be clarified. Nevertheless, the primary objective is to enhance the digital economy, education, e-commerce, and network development (De, 2025). The continent now has 590 million registered internet users, demonstrating the improving trend of Africa's digital transformation (INTERPOL, 2025). Moreover, in 2024, mobile data usage has increased to 75%, and usage of mobile financial services has risen to 85% (Enovise Group, 2024). WhatsApp usage at work has also continued to grow (93%), which could blur the boundaries between personal and workplace data security (Collard, 2025). According to the indegree centrality list[7], China disseminates its technologies most notably through South Africa, Morocco, Algeria, and Egypt (Rojo, 2023).

Huawei, ZTE, and Alibaba are major players in Africa's digitalisation. The inflow of Chinese companies has significantly increased telecommunications coverage in Africa. By 2023, Huawei built 50% of the 3G networks and 70% of the 4G networks in the sub-Saharan region (Kluiver, 2025). This growth is closely linked to the significant presence of Chinese companies, whose comprehensive offerings (comprising hardware, implementation, and financing)[8] facilitated a substantial expansion in 3G coverage across Africa, from 22% in 2010 to 83% in 2023 (Arnold, 2024, GSMA, 2023). However, the digital divide remained significant. The percentage of the population with online access was 43% in 2023, with a more notable increase in more developed countries (Kenya: 83%, Nigeria: 60%, South Africa: 56%) (Enovise Group, 2024). China has pledged to develop digital infrastructure, including by establishing Digital Technology Cooperation Centres and Digital Education Centres to support the AfCFTA (African Continental Free Trade Area) digital trade protocol (Kluiver, 2025).

Based on an analysis of patent networks, China has become the leading technology exporter in Africa, and by 2021, its outdegree centrality[9] (the extent of technology exports) already exceeded the level of the United States (Rojo, 2023). The United States seeks to counterbalance this but is less assertive in terms of investment. While the U.S. remains technologically

[6] China exports surveillance and censorship technologies — often referred to as 'digital authoritarianism' — and actively supports the expansion of state control (Umejei, 2022).
[7] It shows which countries are the biggest technology importers.
[8] China exports not only technological tools but also legal and political models. Its provision of digital infrastructure often comes as a package encompassing hardware, software, and an underlying political framework (Bagwandeen, 2022).
[9] This shows how active a country (in this case, China) is as a technology exporter.

competitive, its presence on the continent is less visible (Dinika, 2022). It is less active in the provision of ICT-based aid in Africa (Mudau, 2022). The US demonstrates comparative strength in the sphere of software and digital platforms (such as Zoom, Google, and Facebook) yet maintains a relatively limited physical presence. The continent represents not only a market, but also a strategic arena between the two major powers (Chitanga, 2022). China maintains a dominant position in infrastructure development (e.g., telecommunications networks, surveillance systems). The United States increasingly approaches Africa from a digital security perspective, aiming to constrain the expansion of Chinese influence (Matanda, 2022).

3.1. The Risks of Technological Dependence

A substantial share of Africa's digital infrastructure is owned or operated by foreign corporations, particularly from China and the United States. Cloud services, data centres, and telecommunications networks are often managed outside African jurisdiction and control (Venske, 2022). Most data on African citizens are collected and stored by foreign platforms (e.g., Google, Meta, Chinese applications), raising legal, security, and economic concerns (Gopaldas, 2022). Loans and financial packages linked to Chinese digital development – particularly through technology transfers tied to loans – could increase countries' debt burdens and financial instability. Chinese funding could lead not only to economic control but also to geopolitical influence, as excessive dependence makes countries vulnerable to political and economic pressure. The deployment of Chinese infrastructure represents a rapid development opportunity for many African countries; however, it also carries technological dependency and data sovereignty risks (Krukowska, 2024). The technologies offered by Chinese suppliers (e.g. Huawei) enable China to indirectly influence the digital infrastructure and data flows of African countries. Through China's Safe City[10] projects, AI-based facial recognition systems, BeiDou satellite navigation and digital surveillance systems, Beijing can gain access to African information and communication networks (Cannon, 2025, Nelson, 2024). Chinese infrastructure could threaten the digital sovereignty of African countries, as technological dependence and a lack of data sovereignty result in a loss of control (Agbebi, 2022). For example, it has been claimed that the Chinese technology giant Huawei has been transmitting data to Chinese servers in Shanghai on a daily basis for the past five years, through computer and telecommunications systems installed at the African Union headquarters in Addis Ababa (Meservey, 2020).

Vulnerabilities in the systems and devices of Chinese companies (Huawei, ZTE) and the ability to control data flows pose a risk of espionage, influence operations, and cyberattacks. Chinese tech giants not only provide infrastructure to countries but also have the potential to provide access to government surveillance systems. The two mentioned Chinese technology companies, been accused of monitoring digital

[10] Safe City projects involve the use of Chinese technologies that introduce advanced surveillance systems. Although these projects bring technological advances, there are concerns about the protection of civil and political liberties (Labscon, 2023).

communications and exerting influence over them. For instance, during periods of political instability in Zimbabwe, the government has imposed internet restrictions, prompting concerns about the involvement of foreign technology providers in facilitating such measures (Labscon, 2023). Planned internet shutdowns are becoming increasingly common, particularly during elections or periods of political unrest, as seen in Ethiopia, Uganda, and Sudan. Such measures are often aimed at suppressing protests and preventing the spread of information (Umejei, 2022).

> *Note: Several countries, such as Kenya and South Africa, have already taken steps to strengthen their digital sovereignty (Venske, 2022). South Africa's preparation for the Fourth Industrial Revolution also serves as a means of mitigating external influences, particularly in the context of the technological rivalry between China and the United States. The government has established a national 4IR commission, which has put forward strategic recommendations for building a 'future-proof' economy. The aim is for the country to become not only a consumer but also a producer of technology (Ndzendze, 2022). But many African countries are unable to adopt alternatives to Chinese technology giants, due to both technical and financial constraints (Mboya, 2022).*

China's dominance in hardware and software, state-backed loans, and lack of transparency in data management could limit technological autonomy and raise sovereignty risks. Over-reliance can make countries vulnerable to political and economic pressure. Furthermore, authoritarian practices may be adopted, such as stricter state control of data and content regulation (Brickstone, 2024).

4. Cyber Capabilities in Africa

In Africa, legal and technical protection significantly lags behind the level of threat. The rapid expansion of the internet, mobile technology, and fintech in many African countries has outpaced the development of appropriate laws, data protection regulations, and digital rights, leaving gaps in areas such as cybersecurity legislation, data protection statutes, and digital trade regulation (Wekesa, 2022). According to INTERPOL, 75% of countries consider their legal, regulatory and enforcement capabilities to be inadequate, and 95% report an insufficient training and resources. In most countries, there is a lack of appropriate incident reporting systems, digital evidence storage and common standardisation. However, many countries have adopted new legislations and strategies, and cooperation at a regional level is also strengthening. (e.g. INTERPOL Serengeti and Red Card operations) (INTERPOL, 2025). In recent years, there has been some progress regarding the establishment of cybersecurity institutions. The Malabo Agreement (on cybersecurity and data protection) – adopted as part of the African Union's digital transformation strategy – and the Cyber Capacity Building Agenda provide significant regional coordination and funding. AFRIPOL-Interpol collaborations (such as training courses on combating cybercrime held in Mauritius) also contribute to practical capacity building. The private cybersecurity sector was valued at USD 2.5 billion in 2020, which is expected to reach USD 3.7 billion by 2025 (Kearney, 2023).

Note: For comparison, the European market is valued at USD 63.12 billion in 2025 (Mordor Intelligence, 2025).

According to the 2024 Global Cybersecurity Index by the International Telecommunication Union (ITU), most countries in Africa are considered to be at the 'evolving' or 'establishing' level. Only seven countries (Mauritius, Tanzania, Rwanda, Ghana, Kenya, Egypt and Morocco) have achieved the highest Tier 1 level. These countries stand out due to their comprehensive legal, technical, organisational and awareness programmes, and because they have functioning Computer Emergency Response Teams (CERTs) and engage in regional cooperation (Chacha and Barclay, 2024, Ecofin Agency, 2024). By international standards, Africa remains far behind. In Europe, 19 countries are classified as Tier 1, including Denmark, Finland, Portugal, Spain, the United Kingdom, Germany, Belgium and Estonia, the latter of which is the most developed country in Europe (International Telecommunication Union, 2024). The US and Canada are considered the most advanced internationally. However, Brazil, India, Japan, South Korea, Australia, Malaysia and Oman are also ranked first[11] (ITU, 2024). Although cybersecurity capabilities in Africa are improving remarkably, most countries still have weak cyber defence (Nelson, 2024). According to Cisco's 2025 Cybersecurity Readiness Index, only 5% of South African businesses consider themselves to be adequately prepared to face modern cyber threats (Cisco, 2025). Although South Africa has the Cybercrimes Act[12] and the Protection of Personal Information Act (POPIA)[13] in place, enforcement and the protection of critical infrastructure (such as health, energy and government systems) remain a serious risk due to a lack of skilled personnel (Caldwell, 2025, MANCOSA, 2025). On the other hand, the growing financial inclusion and expansion of internet access have also significantly increased the attack surface (Wolfenden, 2025, Expression Africa, 2025). The risk of cyber-attacks is further increased by the fact that many African countries are experiencing political transitions, coups, elections, insurgencies and weak IT infrastructure, as well as inadequate security, which factors make the countries more vulnerable to external influence (Nelson, 2024).

5. Cyber Operations in the Region

The development of digital infrastructure in Africa significantly widens the scope for cybercrime. According to the Interpol Africa Cyberthreat Assessment Report 2025, cybercrime currently accounts for 30% of reported crimes in West and East Africa (INTERPOL, 2025). Figure 3 presents a heatmap ranking different types of cybercrime across African regions.

[11] Hungary is rated Tier 2, as 'Advanced' in the ITU 2024 assessment with a score of 88.7. It has relatively advanced capacities (legal framework, operational CERT, technical and organisational foundations) but has not reached the highest level (International Telecommunication Union, 2024).
[12] The Cybercrimes Act in South Africa is a law that criminalizes various online offenses, such as hacking, cyber fraud, and the unlawful sharing of data, to improve cybersecurity and protect individuals and organizations from digital crimes (Cybercrimes Act, 2025).
[13] It is a comprehensive data protection law that governs how personal information must be collected, stored, processed, and shared in South Africa.

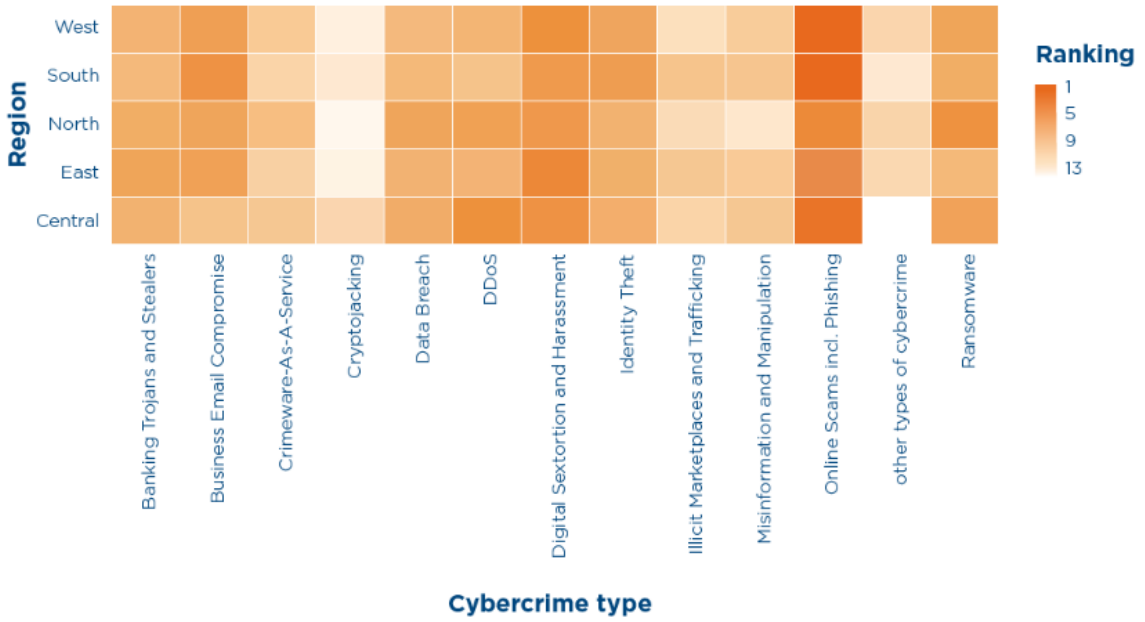

Figure 3: Average ranking of different types of cybercrime by their financial impact across African regions, based on data from INTERPOL member countries
Source: INTERPOL (2025)

Generally, the most common attack methods target the more developed regions of Africa. These methods include phishing, which accounts for 34% of cybercrime on the continent. The effectiveness of phishing and other social engineering campaigns is enhanced by the creation of deepfake content using artificial intelligence tools[14] (Enovise Group, 2024). Ransomware attacks are becoming more frequent, mainly affecting critical infrastructure, banks, and healthcare organisations. Business email compromise (BEC) is also a serious threat (especially in the West African region, where fraudulent emails are causing millions of dollars loss to companies). In addition, there are increasing cases of digital extortion, sextortion campaigns[15], as well as online scams (Enovise Group, 2024). Ransomware attacks were particularly common in South Africa and Egypt, while BEC posed a more serious threat in West Africa (Walsh, 2025, Protectionweb, 2025). In addition, botnets play a significant role in denial of service (DDoS) attacks and data theft (Enovise Group, 2024). In terms of data theft activities, attacks using spyware rose by 14% while password stealers resulted in 26% more incidents detected (Kaspersky, 2025a). According to a Kaspersky report, a total of 131.6 million web attacks were detected in Africa in 2024. The countries experiencing the highest number of attacks were Kenya (20 million), South Africa (17 million), and Morocco (12.6 million) (Kaspersky, 2025b).

The financial sector was the most exposed to attacks. The success of these activities is largely due to the low security awareness of users, the rapid proliferation of mobile banking and payment platforms, and the vulnerability of devices. The African financial sector is currently facing significant cyber threats, particularly from organised criminal groups and state-sponsored

[14] By 2027, it is predicted that the damage caused by attacks with deepfake will exceed $40 billion, representing a rapidly growing threat (Investec, 2024).
[15] According to the report, cases of digital sextortion have increased significantly, particularly in Nigeria, where more than 63,000 Instagram accounts were deleted by mid-2024. Attackers often use explicit content generated by artificial intelligence to extort money (Bagwe, 2025).

actors carrying out high-value thefts. These attacks often exploit vulnerabilities that have previously been targeted, such as weaknesses in payment processes and internal security controls. Attackers can manipulate the integrity of payment systems by exploiting security weaknesses, enabling them to make illegal payments. Financial institutions in Africa are currently facing a significant number of espionage and data theft attempts by state actors, organised crime groups, insider threat actors and individual hackers. In addition, as more third-party service providers (such as fintech firms) become involved in financial infrastructure, the supply chain becomes more vulnerable, expanding the overall attack surface. Furthermore, public administration and e-government portals, the energy sector, and the healthcare and manufacturing sectors are also frequently targeted. Due to their critical importance, telecoms and technology companies are also high-value targets (World Bank Group, 2022).

Given the digital developments, the trends affecting Africa are closely aligned with cyberspace trends observed in the international environment. The extent and severity of these trends depend on the country's systems, the sensitivity of the stored data, and its usability. Motives related to financial profit are not the only drivers of the attacks on the financial sector. Significant foreign investment flows into Africa are also likely to be a contributing factor. The continent's growing geopolitical importance could result in additional state actors focusing their attention on Africa, thereby increasing targeted cyber espionage.

The internet and digital technology have radically changed the way states gather information. Espionage in cyberspace, whether carried out by secret services or other state actors, enables information to be collected and extracted efficiently and without detection. This change extends traditional power relations into the digital dimension, generating a new form of geopolitical competition on the continent in which China is a prominent actor (Africa Center for Strategic Studies, 2025).

5.1. APT Activities

Nowadays, political disagreements and armed conflicts have become an integral part of cyber warfare, with cyber threat actors linked to states carrying out information gathering and espionage operations in line with the underlying interests of the state behind (Arnold, 2024).
APT activity is expected to become increasingly active in Africa by 2024, particularly in the government, energy, and telecommunications sectors. Groups such as MuddyWater[16], FruityArmor[17], and SideWinder[18] use a variety of methods and tactics, including spear phishing, modular malware (DeadGlyph, StealerBot), and the use of legitimate tools and cloud platforms, to increase the effectiveness of their operations. Their motivations are primarily linked to espionage, sabotage or financial gain, which can be attributed to Africa's growing geopolitical and economic importance (Kaspersky, 2025c).

[16] MuddyWater is a cyberespionage group that operates under the Iranian intelligence service, specifically the Ministry of Interior (MOIS) (Mitre Att&ck, 2025).
[17] The cyberespionage APT group mainly focused its operations on organizations in the Middle East (Kaspersky, 2025d).
[18] SideWinder is a highly active and persistent threat actor that continuously evolves and enhances its toolkit. This is a highly prolific APT group that has primarily targeted military and government organizations in Pakistan, Sri Lanka, China, and Nepal, while in Africa, its main targets have been Egypt and Djibouti (Dedola and Berdnikov, 2025).

Given the fact that the African continent is of strategic importance to several major powers (the United States, Russia and China), there is a correspondingly high number of operations aimed at intelligence gathering and espionage, in line with the interests of the underlying country.

Case studies:

1. Diplomatic Specter

The Chinese APT group 'Diplomatic Specter' has been actively targeting government, military and diplomatic institutions in Africa, the Middle East and Asia since late 2022. The group mainly targets foreign ministries, military organisations and embassies (Nelson, 2024).

The group carries out automated daily keyword searches on topics related to diplomacy, military, energy and geopolitics. It uses the sensitive documents and emails obtained to support China's strategic objectives and gain information advantage in international negotiations and by geopolitical efforts (Rochberger and Frank, 2024).

These attacks are directly associated with China's growing political, economic and military presence in Africa and the Middle East. China is making significant economic investments in these regions, primarily in infrastructure and raw materials. The country is also building political alliances and strengthening its military presence, for example, through participation in UN missions and arms sales, while striving for digital dominance. The group is constantly active. Despite being excluded from the networks of some institutions, they continue to operate unhindered elsewhere. They encounter minimal resistance as they often target institutions in politically unstable or less democratic states. This allows attackers to access confidential foreign policy and military decisions, which could have serious consequences for national security (Nelson, 2024).

Operation Diplomatic Specter is a systematic, state-sponsored espionage campaign targeting regions of interest to China in order to gather geopolitically valuable information. This is not a single incident, but a well-established and persistent Chinese cyber sabotage strategy that deliberately collects information from governments, diplomatic, and military targets. Gaining information advantage and building political, economic and military influence through digital infrastructure is an integral part of China's long-term global strategy (Rochberger and Frank, 2024).

2. Sharp Panda

In 2024, China-linked cyberspace actor Sharp Panda attacked several African and Caribbean governments as part of an ongoing cyber espionage campaign. The actor used compromised high-ranking Southeast Asian email accounts to send phishing emails. Chinese cyber threat actors are conducting long-term strategic operations against key industrial sectors in Africa, namely telecommunications, financial institutions, and government entities. These campaigns are closely aligned with China's regional technological ambitions, particularly the Digital Silk Road (DSR) initiative announced in 2015. As part of the cyber-attacks, China is using proxy networks ('operational relay box networks') to obfuscate the origin of attacks, enabling them to gain and maintain access to high-value networks more effectively (Lakshmanan, 2024).

3. BackdoorDiplomacy

Chinese state-sponsored actors – including APT41 and BackdoorDiplomacy, which is closely linked to APT15 – have been carrying out coordinated attacks against African telecommunications, financial, and government institutions for years, supporting Beijing's soft power ambitions[19] in the region (Kovacs, 2023).

The attacks identified by SentinelOne are not only aimed at obtaining confidential information, but also at gaining a competitive advantage and securing technical access that can be used for further intelligence purposes, providing diplomatic and economic advantages to China (Hegel, 2023).

This tendency is further reinforced by the significant presence of Chinese companies, particularly Huawei and ZTE, across the continent. Through large-scale investment, these firms ensure that Africa remains heavily reliant on Chinese telecommunications infrastructure.

BackdoorDiplomacy is active in several African countries, including Kenya, South Africa, Senegal and Ethiopia. Reuters recently reported that the group had carried out attacks on Kenyan government agencies, possibly with the intention of gathering information about debts owed to China (Hegel, 2023, Kovacs, 2023).

4. Operation Tainted Love

Operation Tainted Love is an operation launched in March 2023 by Chinese state actors targeting telecommunications service providers in the Middle East and North Africa. In the case of a North African firm, cyber intrusions occurred concurrently with expansion negotiations, suggesting the intent was to acquire sensitive internal data (Hegel, 2023).

5. Other cases, groups

- SideWinder (also known as T-APT-04 or RattleSnake) is a China-linked cyber threat actor active since 2012, that is active since 2012. The group originally focused on South Asia but now has expanded its activities to Africa and the Middle East, where it carries out attacks against government, military, telecommunications, nuclear, logistics, and shipping targets for strategic intelligence purposes (African Business, 2024).
- Daggerfly (also known as Evasive Panda or Bronze Highland) is an advanced cyber threat, whose activity against African telecommunications companies has been observed since November 2022. The PlugX loader also appeared in the campaign, which was typically used by APT groups with ties to China (Threat Hunter Team, 2023).
- Information gathering operations are often focused on companies in the telecommunications sector, as they can be used to access end-user communications.
- Other China-linked actors, such as FamousSparrow and Earth Estries, are also active on the continent (Hegel, 2023).

[19] Soft power tools do not coerce, but rather 'attract'. China uses these tools to shape Africa's political and economic decisions in the long term without entering into open conflict. These efforts complement hard power and provide China's strategic advantage in the global competition.

The targeted operations carried out by the groups behind the attacks clearly indicate that China's use of cyberspace is a deliberate part of its geopolitical strategy on the continent. The objective of the attacks extends beyond simple system disruption. They are primarily aimed at strategic intelligence gathering intended to support China's geopolitical, nuclear, and military decision-making processes.

5.2. Hacktivist Activities

In Africa, hacktivist activities most often target government, military, electoral and media systems, as well as large corporations. The motivations are linked to political, ideological or anti-corruption agendas, human rights issues, actions against social inequalities, in response to local and regional events. Attacks frequently appear in the form of distributed denial-of-service (DDoS) attacks, data leaks, website defacement or social media campaigns.

- In July 2023, the hacktivist group Anonymous Sudan[20] conducted a large-scale distributed denial-of-service (DDoS) attack targeting Kenya's digital infrastructure, resulting in significant disruptions to government services (including the e-Citizen portal), public utilities, and financial institutions. The attackers claimed political reasons for their actions, accusing Kenya of interfering in Sudanese internal affairs (Kitili and Abiero, 2023).
- On 6 February 2024, the hacktivist group Anonymous Sudan conducted a series of DDoS attacks against Uganda's largest telecommunications providers (Airtel, MTN and Uganda Telecom). The group claimed that the attacks were a form of protest against the companies' alleged support for the Sudanese government in the civil war (Michael, 2025).
- In June 2024, the globally active hacktivist collective Anonymous issued a public warning to the Kenyan government, indicating the likelihood of impending cyberattacks. In its statement, the group criticised the government for corruption and for perceived injustices and abuses in public services (ITEdgeNews, 2024).

Hacktivist activities in Africa are primarily an expression of political disagreement or social tension. Although these actions may cause temporary disruption, they usually do not result in long-term or substantial damage. These activities are attempts to attract attention carried out by cyber threat actors who are not affiliated with any state. They spread their ideology and political messages through social media and various other online platforms.

5.3. Other Influence in the Region

Digital platforms – social media, messaging services – are not only used for intelligence gathering, but also for structured disinformation campaigns. This could undermine the legitimacy of the elections, increase social polarisation, and enable external actors – states or movements – to

[20] There are considerable debate and uncertainty surrounding the activities and background of the Anonymous Sudan group, but a growing number of cybersecurity analyses suggest that the group is likely linked to Russian interest groups or at least cooperates with them. Although they claim to be Sudanese hacktivists, several analysts suggest that their methods, infrastructure, communication channels (e.g., Telegram) and choice of targets are similar in many ways to the activities of pro-Russian hacker groups (e.g., Killnet) (Cloudflare, 2025).

influence the political landscape in the Sahel and West Africa (Africa Center for Strategic Studies, 2025).

For example, in 2024, an advanced APT group with links to India (SideWinder) conducted a series of intense attacks against entities of strategic importance in the Middle East and Africa. The targets of the attacks include government and military agencies, logistics and infrastructure firms, telecommunications providers, financial institutions, universities, and oil trading companies[21] (Lakshmanan, 2024).

Disinformation, monitoring, traffic control, censorship

The 'African Initiative' is a disinformation network with ties to Russia that has operated in West Africa. Its aim is to disseminate false narratives on public health and other issues in order to advance Moscow's political influence in the region (Reuters, 2025).

African peacekeeping missions present further opportunities for the disruption and escalation of information operations. UN peacekeeping operations have been targeted by a number of disinformation campaigns, notably in the Central African Republic (MINUSCA), Mali (MINUSMA) and the Democratic Republic of the Congo (MONUSCO). These often falsely accuse peacekeepers of arms trafficking, supporting terrorists and exploiting natural resources. The disinformation campaign aimed to undermine the international presence of the United Nations by spreading distrust and social tension (in which lack of information played a significant role) (Trithart, 2022).

> *Note: It shows that the internet is not solely a channel of communication, but also a tool of geopolitical and societal influence. Dominance over the digital domain is becoming an increasingly important strategic objective (Umejei, 2022). This is illustrated by the active 'digital battle' between the United States and China on social media platforms (e.g., Twitter, Facebook) aimed at influencing public opinion in Zimbabwe, as part of the broader global soft power competition (Mare, 2022).*

Although the exact source of the disinformation is unclear, it most likely originated from local non-governmental organisations (NGOs) or media outlets with possible links to Russia (e.g. the Wagner Group collaborated with local allies to spread fake news and false information on social media) (Trithart, 2022). Russia's isolated internet infrastructure, known as the Runet, may serve as a model for African states, where state-controlled censorship and ISP-level traffic filtering (using TSPU devices capable of blocking VPN) could also be implemented. Russia exports these censorship and surveillance technologies to African countries, particularly to authoritarian regimes with conservative structures, such as the Central African Republic, Mali, Burkina Faso, and Niger (Rio, 2024).

6. Summary

In recent years, China has emerged as a key contributor to Africa's digital development. The country has provided significant infrastructure, financial and technological support to African

[21] Among the nations previously targeted by the SideWinder are Bangladesh, Djibouti, Jordan, Malaysia, the Maldives, Myanmar, Nepal, Pakistan, Saudi Arabia, Sri Lanka, Turkey, and the United Arab Emirates. In addition, the group has also conducted attacks against diplomatic entities in Afghanistan, France, China, India, Indonesia, and Morocco (Lakshmanan, 2024).

countries, leading to a surge in internet and mobile communications coverage. However, this rapid development entails significant trade-offs, including increased technological dependence and heightened risks to data sovereignty. The digital autonomy of African countries is decreasing as Chinese devices and platforms become more widespread, given that China maintains significant control over data flows, communication networks, and critical infrastructure. This dependency leaves African states vulnerable to economic, political and regulatory pressures, while their levels of indebtedness continue to rise.

The security implications of China's technological presence are also substantial. Although systems such as Safe City platforms, facial recognition cameras and Chinese software solutions help local governments combat crime, at the same time, they also create opportunities for China to conduct surveillance and gain access to data and communications. Such developments further strengthen China's geopolitical and intelligence advantage in Africa while undermining the countries' informational sovereignty and technological autonomy.

As digital development advances, Africa is also experiencing the growing impact of cybercriminal activity, in line with global trends. China's growing digital presence and influence have led to social and political debates in several countries regarding data protection, digital sovereignty, censorship and the use of Chinese surveillance technologies. These issues have rather civil society, international legal and political implications. Recent hacktivist activities in Africa have primarily been linked to local political conflicts, corruption, human rights issues, elections and broader geopolitical tensions. Chinese digital and political influence in Africa is not primarily expressed through hacktivism, but rather through state-led economic and diplomatic instruments, as well as espionage and information operations, many of which are attributed to advanced Chinese cyber threat actors. These attacks have primarily targeted governmental, telecommunications, financial, and diplomatic institutions across Africa, with the primary objective of acquiring sensitive information and advancing economic and political influence.

In the short term, China's digital expansion supports Africa's modernisation. However, in the long term, it poses a significant threat to the continent's digital sovereignty, security and autonomy. In this long-term perspective, China's technological expansion and the increasing digital reliance of African countries not only pose risks to information security and sovereignty but could also contribute to a broader geopolitical shift across the continent. Africa's future is increasingly becoming a focal point of technological, economic, and political rivalry among major powers. Overall, this highlights the importance of African countries diversifying their technological partnerships, strengthening their defence capabilities and developing a more deliberate regulatory framework to reduce their reliance on external actors.

7. Geopolitical Conclusions

The advancement of Africa's digital landscape has been significantly influenced by external support, which has played a crucial role in enabling the continent to achieve its current level of technological progress (most notably China's investments). While the support has been instrumental in reaching the continent's present stage of digital advancement, the direction of development remains asymmetric, creating long-term dependency traps, structural exposure, and the risk of digital exploitation. The economic, demographic, and geopolitical weight of the African continent makes permanent subordination to any global power incompatible. Theoretically, the continent has the capacity to function as an active and equal participant in global affairs. However, the current geopolitical and economic dynamics of the world order

impose constraints on this potential. Foreign resources remain essential for further development; nevertheless, subordination is not inevitable, provided that Africa can strategically and deliberately shape its own digital and political ecosystems over the long term. With its natural resources, market scale, demographic trends, and strategic location, Africa holds considerable geopolitical weight that should allow it to participate as an autonomous and equal actor in the digital domain. In practice, however, weak institutions, political instability, insufficient digital capabilities, and limited domestic investment maintain its structural dependency. External engagements frequently overlook Africa's specific needs and local realities. Escaping dependency traps and limiting exploitation will require a sustained, coordinated, and regionally driven strategy – building on frameworks such as the African Union and the AfCFTA – to empower the continent to shape its digital and political ecosystems according to its own priorities. In addition, building a multipolar partnership model that promotes diversified cooperation would enhance bargaining power and help mitigate exposure.

Author Contributions

All sections of this study were undertaken by the author.

Notes on Contributor

Noémi Csunyó is a researcher and PhD student at the institute of World Economy and International Relations, University of Debrecen, Hungary. Her research interests include world economics and geopolitics. The field of research mainly focuses on the effects of political actions on economic relations (especially between major powers like the US and China). She is also particularly interested in studying the risks of cyber operations and the use of artificial intelligence. In addition, their effect on geopolitical conflicts.

Conflict of Interest

The author hereby declare that no competing financial interest exists for this manuscript.

References

Africa Center for Strategic Studies. (2025). *Understanding Africa's Emerging Cyber Threats*. Africa Center for Strategic Studies. Retrieved August 10, 2025 from https://africacenter.org/programs/cyber/?utm

African Business. (2024). *Kaspersky identifies SideWinder Advanced Persistent Threat (APT) expanding attacks with new espionage tool*. Retrieved August 10, 2025 from https://african.business/2024/10/apo-newsfeed/kaspersky-identifies-sidewinder-advanced-persistent-threat-apt-expanding-attacks-with-new-espionage-tool

Agbebi, M. (2022). *China's Digital Silk Road and Africa's Technological Future. Council on Foreign Relations*. Council on Foreign Relations (CFR). Retrieved August 10, 2025 from https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf

Arnold, S. (2024). *Africa needs China for its digital development – but at what price?* Retrieved August 10, 2025 from https://world.edu/africa-needs-china-for-its-digital-development-but-at-what-price/

Article 19. (2024). *China-Africa Cooperation: Beijing's vision raises free expression concerns*. Retrieved August 10, 2025 from https://www.article19.org/resources/china-africa-cooperation-beijings-vision-raises-free-expression-concerns/

Ayodele, O. (2022). *US's and China's 'chipageddon' hits Africa's digital transformation mission*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/us-and-chinas-chipageddon-hits-africas-mission-to-build-digital-economies/

Bagwandeen, M. (2022). *China expands its digital sovereignty to Africa*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/china-expands-its-digital-sovereignty-to-africa/

Bagwe, M. (2025). *Africa Faces a Digital Sextortion Crisis as Numbers Surge Across the Continent*. Retrieved August 10, 2025 from https://thecyberexpress.com/africa-faces-a-digital-sextortion-crisis/

Brickstone. (2024). *The Hidden Costs of China's Digital Ambitions in Africa: Are We Ready for the Consequences?* Retrieved August 10, 2025 from https://brickstone.africa/the-hidden-costs-of-chinas-digital-ambitions/

Caldwell, A. (2025). *South Africa's Digital Future Undermined by Growing Cyber Threats*. Retrieved August 10, 2025 from https://informationstreamer.com/2025/03/20/south-africas-digital-future-undermined-by-growing-cyber-threats/

Cannon, B. J. (2025). *Maps showing China's growing influence in Africa distort reality – but some risks are real*. The Conversation. Retrieved August 10, 2025 from https://theconversation.com/maps-showing-chinas-growing-influence-in-africa-distort-reality-but-some-risks-are-real-249454

Chacha, L., & Barclay, C. (2024). *Mapping Africa's Cybersecurity Development - Insights from the Global Cybersecurity Index 2024*. DPO Caribbean.

China Africa Research Initiative. (2025). *Chinese FDI in Africa Data Overview*. Retrieved August 10, 2025 from https://www.sais-cari.org/chinese-investment-in-africa

Chitanga, G. (2022). *Wired Africa now Zooms into China and US*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/wired-africa-now-zooms-into-china-and-us/

Cisco. (2025). *2025 Cisco Cybersecurity Readiness Index: Readiness remains flat as AI transforms the industry*. Retrieved August 10, 2025 from https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index.pdf

Cloudflare. (2025). *What is Anonymous Sudan?* August 10, 2025. https://www.cloudflare.com/learning/ddos/glossary/anonymous-sudan/

Collard, A. (2025). *African Cybersecurity & Awareness Report 2025*. KnowBe4 Whitepaper. Retrieved August 10, 2025 from https://www.knowbe4.com/hubfs/Africa-Annual-Survey_Whitepaper_US_EN-F.pdf#prId=332108

Cybercrimes Act. (2025). *The full text of the Cybercrimes Act in South Africa*. Retrieved August 10, 2025 from https://cybercrimesact.co.za/

De, R. (2025). *China-Africa Relations: Debt and Investment – Are there new models for engagement?* Finance for Development Lab. Retrieved August 10, 2025 from https://findevlab.org/china-africa-relations-debt-and-investment-are-there-new-models-for-engagement/

Dedola, G., & Berdnikov, V. (2025). *SideWinder targets the maritime and nuclear sectors with an updated toolset*. Retrieved August 10, 2025 from https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

Dinika, A. A. (2022). *ICT investments: Africa waits to see the money*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/us-china-ict-investments-implications-for-africas-socioeconomic-development/

Ecofin Agency. (2024). *ITU Names 7 African Nations Among Top Cybersecurity Models*. Retrieved August 10, 2025 from https://www.ecofinagency.com/telecom/1709-45902-itu-names-7-african-nations-among-top-cybersecurity-models

Enovise Group. (2024). *The Current State of Cyber Threats in Africa – Insights from the Interpol's 2024 African Cyberthreat Assessment Report (3rd Edition)*. Retrieved August 10, 2025 from https://www.linkedin.com/pulse/current-state-cyber-threats-africa-insights-from-interpols-african-siijf

Expression Africa. (2025). *Over half of Africans fear financial losses from cybercrime – KnowBe4*. Retrieved August 10, 2025 from https://expression.africa/over-half-of-africans-fear-financial-losses-from-cybercrime-knowbe4/

Gariba, A. (2022). *Democracy in Africa: Enter the dragon*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/democracy-in-africa-enter-the-dragon/

Global System for Mobile Communications Association (GSMA). (2023). *The State of Mobile Internet Connectivity 2023: Sub-Saharan Africa key trends*. Retrieved August 10, 2025 from https://www.gsma.com/r/wp-content/uploads/2023/10/State-of-Mobile-Internet-Connectivity-2023-Sub-Saharan-Africa.pdf

Good Governance Africa. (2022). *Africa in Fact. China vs US: the battle for digital supremacy in Africa*. Retrieved August 10, 2025 from https://gga.org/project/issue-62/

Gopaldas, R. (2022). *A theatre for competition*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/a-theatre-for-competition/

Hegel, T. (2023). *Cyber Soft Power. China's Continental Takeover*. SentinelOne. Retrieved August 10, 2025 from https://www.sentinelone.com/labs/cyber-soft-power-chinas-continental-takeover/

Huang, Z., & Pollio, A. (2023). Between highways and fintech platforms: Global China and Africa's infrastructure state. *Geoforum*, *147*, 103876. https://doi.org/10.1016/j.geoforum.2023.103876

International Telecommunication Union (ITU). (2024a). *Estonia ranks fifth in the global cybersecurity index*. Retrieved August 10, 2025 from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx

International Telecommunication Union (ITU). (2024b). *Global Cybersecurity Index 2024*. ITU Publications. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

INTERPOL. (2025). *New INTERPOL report warns of sharp rise in cybercrime in Africa*. Retrieved August 10, 2025 from https://www.interpol.int/content/download/23094/file/25COM009248%20-%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf

Investec. (2024). *Cybersecurity: Trends, threats, and strategy*. Retrieved August 10, 2025 from https://www.investec.com/en_za/focus/money/cybersecurity-in-south-africa-2024.html

ITEdgeNews. (2024). *Kenya on high alert: Hacktivist group Anonymous sends warnings to government*. Retrieved August 10, 2025 from https://www.itedgenews.africa/kenya-on-high-alert-hacktivist-group-anonymous-sends-warnings-to-government/

Kaspersky. (2025a). *14% increase in spyware attacks on African businesses: Kaspersky presents a cyberthreat landscape report at GITEX Africa in Morocco*. Retrieved August 10, 2025 from https://www.kaspersky.com/about/press-releases/14-increase-in-spyware-attacks-on-african-businesses-kaspersky-presents-a-cyberthreat-landscape-report-at-gitex-africa-in-morocco

Kaspersky. (2025b). *Africa Cyberthreat Landscape Report 2025*. Retrieved August 10, 2025 from https://content.kaspersky-labs.com/se/media/en/africa-cyberthreat-landscape-report-2025.pdf

Kaspersky. (2025c). *Cybersécurité: les entreprises africaines face à une hausse préoccupante des attaques, selon Kaspersky*. August 10, 2025). https://www.kaspersky.fr/about/press-releases/cybersecurite-les-entreprises-africaines-face-a-une-hausse-preoccupante-des-attaques-selon-kaspersky

Kaspersky. (2025d). *FruityArmor*. Retrieved August 10, 2025 from https://apt.securelist.com/apt/fruityarmor

Kearney. (2023). *Cybersecurity in Africa – call to action*. Retrieved August 10, 2025 from

https://www.kearney.com/documents/291362523/296371292/Cybersecurity+in+Africa%E2%80%94a+call+to+action.pdf/cb6f42c4-570c-ddd7-4f8c-719507863674?t=1683214143000

Kitili, J., & Abiero, D. (2023). *Kenya's Digital Infrastructure Under Threat? A Look at Anonymous Sudan's Thwarted Cyberattack Attempt and its Implications for Kenya's Digital Systems*. Strathmore University Centre for Intellectual Property and Information Technology Law (CIPIT) blog. Retrieved August 10, 2025 from https://cipit.strathmore.edu/kenyas-digital-infrastructure-under-threat-a-look-at-anonymous-sudans-thwarted-cyberattack-attempt-and-its-implications-for-kenyas-digital-systems/

Kluiver, J. (2025). *China-Africa Investments in 2025: Key Trends and How it can Improve Africa's Competitiveness.* Africa International Advisors. Retrieved August 10, 2025 from https://www.africaia.com/insights/china-africa-investments-in-2025-key-trends-and-how-it-can-improve-africas-competitiveness

Kovacs, E. (2023). *China's Offensive Cyber Operations in Africa Support Soft Power Efforts*. Retrieved August 10, 2025 from https://www.securityweek.com/chinas-offensive-cyber-operations-in-africa-support-soft-power-efforts/

Krukowska, M. M. (2024). China's security relations with Africa in the 21st Century. *Security and Defence Quarterly*, *46*(2), 4-23. https://doi.org/10.35467/sdq/190066

Labscon. (2023). *The Cyber Arm of China's Soft Power: Reshaping a Continent*. SentinelOne. Retrieved August 10, 2025 from https://www.sentinelone.com/labs/labscon-replay-the-cyber-arm-of-chinas-soft-power-reshaping-a-continent/

Lakshmanan, R. (2024). *New Frontiers, Old Tactics: Chinese Espionage Group Targets Africa & Caribbean Govts*. Retrieved August 10, 2025 from https://thehackernews.com/2024/05/new-frontiers-old-tactics-chinese-cyber.html?m=1&

MANCOSA. (2025). *South Africa's digital future hindered by rising cyber threats*. Retrieved August 10, 2025 from https://www.fanews.co.za/article/technology/41/general/1204/south-africa-s-digital-future-hindered-by-rising-cyber-threats/41284

Mare, A. (2022). *Digital diplomacy shootout in Zimbabwe*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/zims-chinese-and-us-embassies-digital-diplomacy/

Matanda, D. (2022). *How the contest for global digital hegemony impacts Africa*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/how-contest-for-global-digital-hegemony-impacts-africa/

Mboya, C. (2022). *No Huawei, no cry*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/no-huawei-no-cry/

Meservey, J. (2020). *Government Buildings in Africa Are a Likely Vector for Chinese Spying*. The Heritage Foundation. Retrieved August 10, 2025 from

https://www.heritage.org/asia/report/government-buildings-africa-are-likely-vector-chinese-spying

Michael, C. (2025). *Top 10 cyberattacks that targeted African organisations in 2024*. Retrieved August 10, 2025 from https://businessday.ng/news/article/top-10-cyberattacks-that-targeted-african-organisations-in-2024/

Mitre att&ck. (2025). *MuddyWater*. Retrieved August 10, 2025 from https://attack.mitre.org/groups/G0069/

Mordor Intelligence. (2025). *Europe Cybersecurity Market Size, Share, Analysis, Trends (2025 - 2030)*. Retrieved August 10, 2025 from https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market

Mudau, P. (2022). *Big-spending China woos Africa with its BRI and DSR*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/chinese-foreign-aid-to-africa-for-ict-implications-for-the-us/

Munyati, C. (2024). *Why strong regional value chains will be vital to the next chapter of China and Africa's economic relationship*. World Economic Forum. Retrieved August 10, 2025 from https://www.weforum.org/stories/2024/06/why-strong-regional-value-chains-will-be-vital-to-the-next-chapter-of-china-and-africas-economic-relationship/

Ndzendze, B. (2022). *South Africa's 4IR strategy*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/south-africas-4ir-strategy/

Nelson, N. (2024). *China APT Stole Geopolitical Secrets From Middle East, Africa & Asia*. Darkreading. Retrieved August 10, 2025 from https://www.darkreading.com/threat-intelligence/china-apt-stole-geopolitical-secrets-from-middle-east-africa-and-asia

Paterson, S. (2024). *How much of China's investment into Africa is real?* Hinrich Foundation. Retrieved August 10, 2025 from https://www.hinrichfoundation.com/research/article/fdi/how-much-of-china-investment-into-africa-is-real/

Prakash, S. (2025). *The Digital Silk Road: China's Technological Engagement in Africa*. Roosevelt-Group. Retrieved August 10, 2025 from https://roosevelt-group.org/quick-takes/the-digital-silk-road-chinas-technological-engagement-in-africa

Protectionweb. (2025). *New INTERPOL report warns of sharp rise in African cybercrime*. Retrieved August 10, 2025 from https://www.protectionweb.co.za/cyber-security/new-interpol-report-warns-of-sharp-rise-in-african-cybercrime/

Reuters. (2025). *UK discovers Russian 'espionage tool', sanctions GRU officers over cyberattacks*. Retrieved August 10, 2025 from https://www.reuters.com/world/uk/uk-discovers-russian-espionage-tool-sanctions-gru-officers-over-cyberattacks-2025-07-18/

Rio, N. (2024). *Russia's offensive on "digital sovereignty" in Africa*. Retrieved August 10, 2025 from https://incyber.org/en/article/russias-offensive-on-digital-sovereignty-in-africa/

Rochberger, L., & Frank, D. (2024). *Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia*. Paloalto Networks. Retrieved August 10, 2025 from https://unit42.paloaltonetworks.com/operation-diplomatic-specter/

Rojo, J. V. (2023). China's technological footprint in Africa: A patent network analysis. *South African Journal of Business Management*, *55*(1), a4331. https://doi.org/10.4102/sajbm.v55i1.4331

Threat Hunter Team. (2023). *Daggerfly: APT Actor Targets Telecoms Company in Africa*. Retrieved August 10, 2025 from https://www.security.com/threat-intelligence/apt-attacks-telecoms-africa-mgbot

Trithart, A. (2022). *Disinformation against UN Peacekeeping Operations.* International Peace Institute. Retrieved August 10, 2025 from https://www.ipinst.org/wp-content/uploads/2022/11/2212_Disinformation-against-UN-Peacekeeping-Ops.pdf

Umejei, E. (2022). *The internet war in Africa*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/the-internet-war-in-africa/

United Nations Trade and Development (UNCTAD). (2025). *World Investment Report 2025*. Retrieved August 10, 2025 from https://unctad.org/publication/world-investment-report-2025

Venske, T. (2022). *Sovereignty and digital transformation in Africa*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/sovereignty-and-digital-transformation-in-africa/

Walsh, M. (2025). *Africa faces cybercrime crisis amid weak enforcement, INTERPOL warns*. Retrieved August 10, 2025 from https://cybernews.com/cybercrime/interpol-africa-cybercrime-forensics/

Wekesa, B. (2022). *Policy, legal and regulatory issues in Africa's digital sphere*. Good Governance Africa. Retrieved August 10, 2025 from https://gga.org/legal-and-regulatory-issues-in-africas-digital-sphere/

Wolfenden, K. L. (2025). *Cybersecurity Concerns Increase in Africa as Mobile Banking and AI Threats Surge*. Retrieved August 10, 2025 from https://techafricanews.com/2025/02/18/knowbe4-report-highlights-digital-risks-in-africa-amid-growing-use-of-technology/

World Bank Group. (2022). *Cyber Threats to the Financial Sector in Africa. An Assessment of the Current Threat and an Analysis of Emerging Trends on the Future Threat Landscape*. Retrieved August 10, 2025 from https://documents1.worldbank.org/curated/en/099830405172214598/pdf/P16477000601530760af01093740e385fe8.pdf