Cyber Soft Power | China's Continental Takeover

sentinelone.com/labs/cyber-soft-power-chinas-continental-takeover/

Tom Hegel

Executive Summary

- SentinelLabs observes sustained tasking towards strategic intrusions by Chinese threat actors in Africa, designed to extend influence throughout the continent.
- New attacks include those against telecommunication, finance and government, attributed to the BackdoorDiplomacy APT and the threat group orchestrating Operation Tainted Love.
- China's engagement in soft power diplomacy has a lengthy history, yet the use of strategic cyber intrusions highlights recent objectives and potential lasting impact in Africa.
- To better manage the challenge of tracking state-aligned cyber activities in less monitored areas like Africa and Latin America, we are announcing the formation of the 'Undermonitored Regions Working Group'. Launched today at LABScon, this effort calls upon established security researchers to join analytic capabilities, combine telemetry, resources, and local expertise, and promote a unified approach to analyzing cyber operations used to support soft power agendas in Africa and Latin America.

Introduction

In the evolving cyber threat landscape, it's always important to constantly challenge our biases. There are large pockets of important threat activity occurring in regions around the world less commonly addressed in Western threat research. While much attention has rightfully been drawn to Chinese threat actors targeting the West, the broader set of global activity supporting and promoting similar interests remains opaque. At a time of pervasive foreign activities towards cornering natural resources and co-opting the governance of less represented countries, we have to ask– what is happening across the vast African continent?

As we contemplate where China might stand in the global arena in the next 5 to 10 years, it's evident that there exists a considerable gap in the realm of cyber threat intelligence with regards to Africa as a whole, and more specifically how it ties into the long term agenda of the People's Republic of China (PRC). Africa, with its highly complex and dynamic environment, poses a unique challenge for accurately characterizing its cyber threat landscape.

In the threat intelligence industry, we have a habit of overlooking regions where our immediate financial interests don't appear to be at stake. Yet, it is precisely in places like Africa and Latin America that we witness these threat actors subtly shifting the balance of

negotiations and playing pivotal roles in larger geopolitical strategies. There's an urgent need to acknowledge the importance of these frequently overlooked regions in the global threat landscape and take radical steps to close the gap in our situational awareness. These regions are shaping up to be the battlegrounds of the future.

Our focus is on incentivizing strategic intelligence on the state of cyber operations targeting Africa. We recognize that these operations need to be placed in the greater context of multidimensional campaigns that include more traditional forms of espionage, market maneuvers, and influence. This is vital in understanding the PRC's geostrategic ambitions and technological investments, and are fundamental in forging a forward-thinking and holistic defense approach. We'll highlight key examples including the targeting from Chinese state-sponsored APTs, such as Op. Tainted Love and BackdoorDiplomacy, and how they blend into PRC's soft power agenda across Africa.

Background on Soft Power Engagement

While cyber capabilities are important, they are just one of the more recent tools used in implementing broad national soft power strategies. Spanning several decades, China's involvement in the continent has adapted to embrace economic, political, and cultural dimensions that represent both comprehensive and strategic opportunities. The establishment of Confucius Institutes and expanding media investments have been a tool in crafting narratives that underline the positive aspects of its engagement in Africa.

China has engaged in significant strategic investments in Africa, considered 'debt-trap diplomacy'. This refers to a scenario where a creditor country extends excessive credit to a debtor country with the presumed intention of extracting economic or political concessions when the debtor country cannot meet its repayment terms.

Specifically in Africa, China has financed large critical infrastructure projects in many African countries. Countries pursuing economic and infrastructure development have found China a willing and eager investor over the last decade. Future adverse effects are easily brushed aside by the immediate perceived benefits of these investments.

Offensive Cyber Operations as a Support Tool of Soft Power Agendas

In recent years, we have tracked targeted intrusions against key industrial sectors in various African nations. These attacks conspicuously align with China's broader soft power and technological agenda in the region, focusing on critical areas such as the telecommunication sector, financial institutions, and governmental bodies. Three significant sets of activity best exemplify this dynamic across the larger set of China-aligned activity in Africa.

Operation Tainted Love

In March 2023, we shared details of Operation Tainted Love, a case centered on targeted attacks against telecommunications providers predominantly located in the Greater Middle East region. This discovery marked an evolution of the toolkit involved in Operation Soft Cell, forging immediate connections to previous China-attributed activities.

From Operation Tainted Love, we highlighted the use of a rigorously maintained and version-controlled system for credential theft, accompanied by a novel dropper mechanism. The overall findings are suggestive of a concerted development effort undertaken by a threat actor, or threat actors support structure, driven by specific objectives.

Operation Tainted Love

Unnoted in our initial report, we identified the compromise of a telecommunications entity based in North Africa by the same threat actor. The timing of this activity aligned closely with Chinese telecommunication soft power interests in Africa, as the organization was in private negotiations for further regional expansion in areas. Strategic objectives in such intrusions highlight interest from China in internal business knowledge on negotiations, providing competitive advantage, or prepositioning for retained technical access for intelligence collection.

Backdoor Diplomacy

For several years, another APT primarily referred to as BackdoorDiplomacy has operated across Africa. Recently, fresh revelations emerged spotlighting the group's sustained three-year endeavor targeting governmental organizations in Kenya. Delving into prior public technical reports by ESET, Unit42, and BitDefender unveils a targeting paradigm bearing resemblance to those employed in Operation Tainted Love.

BackdoorDiplomacy seemingly concentrates efforts on government entities, along with high-priority telecommunications and finance organizations. The group has orchestrated a series of notable espionage campaigns across Africa in recent years. Through analysis of infrastructure tied to this actor, we assess multiple African countries are experiencing targeting over the last few years, including at least South Africa, Kenya, Senegal, and Ethiopia. As noted by previous reporting, the threat actor does maintain operations throughout the middle east, and can be found in other regions of particular PRC interest.

Our current perspective suggests a close relationship between BackdoorDiplomacy and another Chinese state sponsored threat actor, APT15.

Threat Actors Ambiguity

A broader set of China-aligned campaigns has been active across Africa, as emphasized by recent reports on FamousSparrow and Earth Estries. Pinpointing precise clustering for these groups remains challenging due to a prevalence of shared technical resources. However, TTPs and targeting objectives are somewhat related to the APT41 umbrella.

In a separate case, Chinese espionage efforts against the African Union (AU) was allegedly discovered in 2017. According to initial reports, for a period of five years, from 2012 to 2017, the Chinese government maintained backdoor access into servers for the African Union's headquarters in Ethiopia. The $200 million dollar headquarters was funded and built by China between 2009 and 2012. Notably, the network infrastructure and services were reportedly Huawei technology since the initial construction.

African Union Headquarters, Addis Ababa

More recently in 2020, Japan's CERT notified AU IT staff of an intrusion they attributed to the Bronze President APT, a separately tracked Chinese threat actor. In this intrusion, Bronze President was observed exfiltrating surveillance footage from the AU headquarters facility. This case may highlight how much of a real priority intelligence inside the AU is to Beijing, ultimately forcing their hand on moving away from backdoored equipment to performing actual intrusions through well tracked APTs.

In both the 2017 and 2020 case, African Union and Chinese officials denied any sort of intrusions. As quoted by Reuters, a former AU official told them "Attacking the Chinese, for us, it's a very bad idea,". A review of specifics around China's technological soft power in Africa highlights some reasons why the official may have said that.

Technological Soft Power, Reliance, and Abuse Opportunities

The digital landscape of Africa has undergone a seismic transformation, largely facilitated through Chinese tech giants deploying extensive resources to meet the continent's critical technological needs.

China has taken a lead role in Africa's telecommunication, finance, and surveillance technology sectors. This initiative ties into China's Digital Silk Road project, announced in 2015.

Telecommunication Networks

At the forefront of technology investment in Africa are Huawei and ZTE, powerhouses steering efforts to bridge the connectivity divide separating urban and rural landscapes of the continent. These corporations have brought the boon of digital connectivity to the remotest corners of Africa.

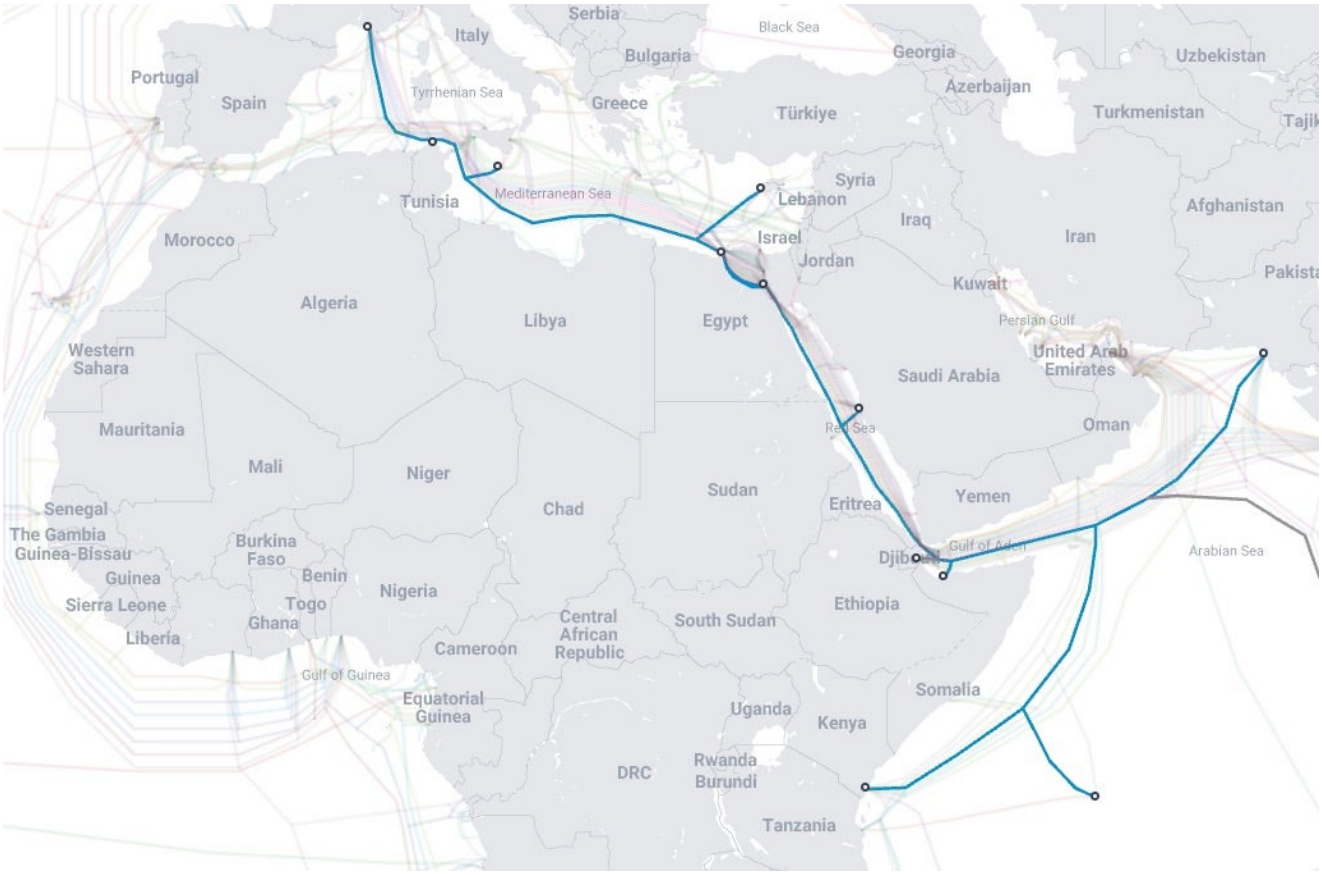
In the two decades since Huawei began expanding into Africa, it has grown to become the leading telecommunication technology and service provider across much of the continent.

Yet, underneath the altruistic veneer may lie a strategy anchored on fostering an overwhelming dependence on Chinese technology. Through a sweeping range of initiatives that span from mobile networks to broadband infrastructure, the strategy envisions a society deeply tied to China's digital ecosystem, guiding future socio-political paths and holding significant sway over personal freedoms.

This rise isn't merely a route to economic enrichment; it empowers China to shape policies and narratives aligned with its geostrategic ambitions, establishing itself as a pivotal and defining force in Africa's digital evolution.Targeted intrusions by the BackdoorDiplomacy APT and the threat group orchestrating Operation Tainted Love indicate a level intention directed at supporting such agendas.

Instances of infringement on internet rights and the misuse of technology are already evident in countries such as Sudan, Ethiopia, Zimbabwe, Gabon, and the Democratic Republic of Congo. In some of these nations, the governments have resorted to shutting down social media and internet services as a strategy to suppress civil unrest, or even spying on the network communications of its citizens.

China has also ventured to enhance its command over the underwater fiber networks connected to the African continent. Leveraging significant investments in projects such as the PEACE cable initiative, China has been laying cables that aim to rejuvenate Africa's digital connectivity, ostensibly offering the continent much needed information accessibility.



Peace Cable Map, TeleGeography

These underwater pathways hold enormous significance in dictating the flow of information between continents. In taking ownership of them, China stands in a position to potentially orchestrate and steer digital dialogues on the African continent, forging a narrative that aligns seamlessly with its geopolitical objectives.

Controlling these undersea networks gives China the capacity to monitor the data flowing through them, raising serious concerns regarding data privacy and national sovereignty. To gauge the potential for misuse, we only need to examine how China manages its own domestic networks, offering a window into the possible ramifications of granting them such control.

Mobile Payment Platforms

In recent years, digital mobile banking platforms like M-Pesa have revolutionized Africa's financial landscape, promoting unprecedented financial inclusion especially in areas underserved by traditional banks. With 51 million users processing over $314 billion in transactions annually, its footprint is substantial.

M-Pesa has since been migrated to Huawei's Mobile Money Platform. Similarly, China-backed entities OPay and PalmPay have seized a considerable market share, facilitating a large portion of the continent's financial transactions.

This should raise apprehensions around the nature of China's influence, with potential avenues for financial monopolies and the control it gives to Chinese stakeholders in the dictation of economic trajectories across the African continent.

The intensive data mining, user surveillance, and user disruption that are characteristic of Chinese tech giants present a significant risk of exploitation, infringing upon the privacy rights of individuals and potentially undermining the sovereignty of African nations. The depth and breadth of data these platforms can amass and control raise serious concerns about how it might be utilized, perhaps to shape consumer behavior, influence public opinion, or even foster dependencies that go beyond financial transactions.

While services offered by these platforms are undeniably bringing about a financial revolution, it's creating a scenario where a foreign power has an overwhelming influence over the financial stability, habits, and preferences of a significant portion of the African populace. Financial inclusion and potential manipulation hang in a precarious balance, necessitating a critical appraisal of the long-term implications of this growing influence.

Surveillance

Huawei's Smart City venture is also emerging as a central pillar in China's escalating soft power influence in Africa. This initiative pivots on a suite of surveillance services including facial recognition, artificial intelligence, data analytics, and 5G network deployments, all purportedly claimed to enhance urban management, augment public safety, and spur economic development. Yet, the flipside of this technological investment is the possibility of a surveillance era of unparalleled scope, exploiting a diverse array of data from daily life to cultivate a society where personal privacy could soon become obsolete.

Across Africa, nations like Kenya, Mauritius, Uganda, and Zambia have embraced Huawei, infusing surveillance technology into the heartbeat of their urban landscapes. In Kenya, the Safe City project — powered by Huawei's system encompassing CCTV and facial recognition technologies — monitors Nairobi and other primary cities. In Uganda, one such case of surveillance reportedly led to the regime seeking to silence political opponent Bobi Wine, accomplished through the help of Huawei staff and services. These same capabilities can be found in many other countries throughout Africa.

Bobi Wine, source: Bloomberg

Other noteworthy activity includes the Chinese business CloudWalk Technology providing facial recognition surveillance technology to Zimbabwe. CloudWalk has been accused of being involved in human rights violations and transgressions perpetrated during China's campaign targeting Uighurs, ethnic Kazakhs, and other Muslim minority groups in the Xinjiang Uighur Autonomous Region. This campaign is characterized by widespread repression, indiscriminate detentions, enforced labor, and intensive high-tech surveillance.

Once these smart cities come to fruition, they will operate fundamentally on Chinese technology, often granting Beijing real-time insights into these nations, lacking consequences for personal privacy and national safeguarding measures. Moreover, these nations steer towards further reliance on Chinese expertise and technical resources for the use and administration of these systems into the future.

A Force for Good

African nations face the delicate task of leveraging Chinese tech innovations while preserving their autonomy and digital rights, a tightrope walk exacerbated by limited alternatives. Concurrently, it's imperative for the cybersecurity community to deepen our understanding of China's cyber activities in Africa to prevent unwanted encroachment.

Due to escalating cyber threats in overlooked areas such as Africa and Latin America, we are launching the Undermonitored Regions Working Group (URWG). This initiative is focused on addressing the unique cybersecurity hurdles faced in these regions, frequently sidelined in mainstream global cyber discussions.

Our mission transcends geographical boundaries as we track state-sponsored threats emerging globally from nations be it China, Russia, or Egypt. We are determined to cultivate a technical research collaboration, harnessing our collective expertise to identify new threats, and devise effective countermeasures against them.

SentinelLabs embodies our commitment to sharing openly – providing tools, context, and insights to strengthen our collective mission of a safer digital life for all. We are seeking out security researchers, intelligence analysts, and those passionate about understanding and improving the cyber threat narrative to grow these efforts through unconventional means. By pooling our knowledge and technical prowess, we strive to nurture a digital future in support of less monitored parts of the world.

Conclusion

As we have navigated through the complexities of Chinese influence in Africa, the role of offensive cyber actions, and the broader implications of tech dominance, it becomes evident that this intricate web of geopolitics and cyber threats demands attention across the cybersecurity industry.

Recognizing Africa's centrality in the future of global cyber dynamics helps not only the safeguarding of the continent's digital freedoms but fortifies the global ecosystem against sophisticated threat actors.

The story of Africa's digital landscape today is, in essence, the precursor to the global narrative of tomorrow. We should work in tandem to craft it as one of security, prosperity, and shared progress.