The GLOCEPS
Weekly Influential Brief
Research And Analysis In Foreign Policy Pillar

Implications of increased foreign surveillance technologies on national security in Africa

Peter Mbuthia

Executive Summary

The adoption of foreign surveillance tools in Africa threatens the continent's security and sovereignty. The instruments have thrived globally through collaborations between intelligence agencies and private companies seeking to address global security matters such as counter-terrorism. While this is applauded in Africa, the use of these technologies has enhanced the conduct of clandestine activities in the continent without due regard to issues, such as data privacy. This has resulted in the race for data collection as the quest to gain advantage in favor of foreign national interests heightens. Subsequently, insufficient cyber security policies have rendered African countries vulnerable to this fast-evolving threat. There is a need for enhanced technological partnerships between states and relevant stakeholders in protecting the continent's cyberspace.

Context

Spyware technology has become a stealthy way for states and non-state actors to gather intelligence beyond the conventional use of human spies. The inability to be detected has been possible through the infusion of artificial intelligence (AI) in manufacturing these surveillance devices. AI-based surveillance operations violate universal and domestic policies safeguarding privacy. Consequently, they are considered a risk to human rights. While it has raised concerns, companies such as Pegasus, Circles and Huawei have continued to manufacture them for their African consumers. Unfortunately, the latter are not taking adequate precautions to safeguard the data collected by these machines.

Even though the African Union convention on cyber security and data protection has established a joint cybersecurity framework for all, only 13 of the 55 AU member states have signed and ratified it. This laxity is due to the opacity of the minimum thresholds of the recommended regulations. Despite Kenya being among the non-signatories, she has put in place cyber security measures, such as creating a data protection commission and a National Computer and Cybercrime Coordination Committee to enhance the domestic protection of her cyberspace. These measures are part of Kenya's national security strategies to exploit its potential in the growing digital economy.

The tools used to conduct illegal surveillance are affordable. They have enabled easy access for malicious individuals and governments seeking to extend the limits of their terms of engagement. Such authoritarian regimes have used the tools to interfere with democratic processes and freedoms through spying on individuals, groups and societies. Governments of Morocco, Nigeria and Zambia have relied on these tools to illegally access calls, texts and even precise device locations linked to their opponents worldwide. All this is possible through platforms such as Circles, a Bulgarian affiliate of Pegasus software.

Photo Credit: African Arguments

Key issues

The following are the effects of foreign surveillance technologies across the African continent.

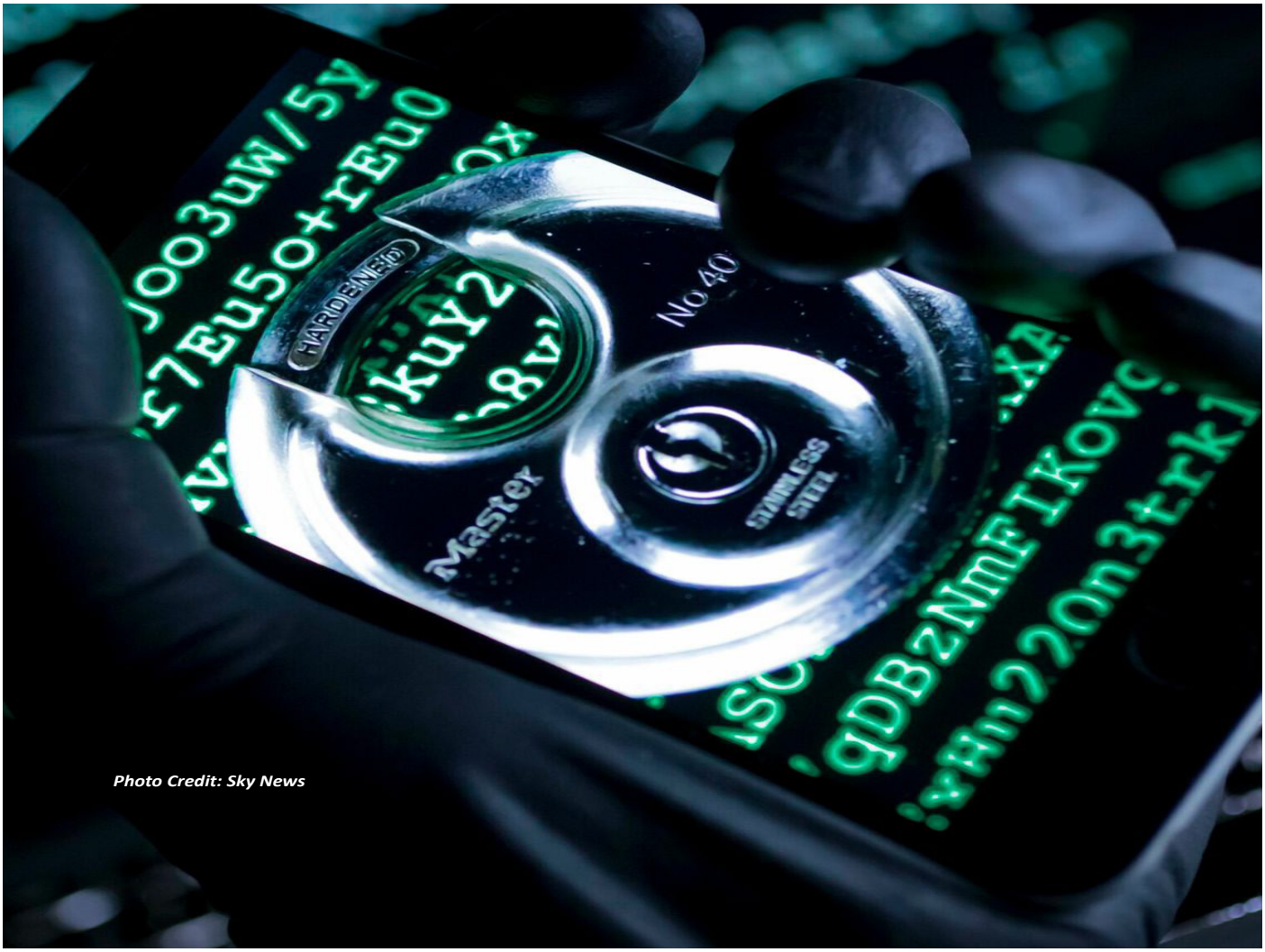


Photo Credit: Sky News

Undermined data privacy

The lack of adherence to data privacy protection among African countries is a threat. Foreign companies contracted to conduct projects beyond their borders act as proxy agents fostering their country of origin's interests and thereby posing a threat to the security of the host state. For instance, cases of the premises of regional bodies, such as the African Union, being hacked and vital information transmitted to Beijing, China, through illegal recordings, have been reported. Elsewhere, the Chinese technology company, Huawei, has been linked to an unlawful intrusion into Australian telecommunications systems for espionage purposes. Such a case is a cause for alarm among African states conducting developmental projects with possibly malicious partners. Africa has lagged behind in terms of regulatory and encryption mechanisms. Consequently, this has led to infringement of the right to privacy as personal data collected through biometrics and on the internet is not protected against misuse. As Africa strives towards digitizing her government systems and essential services by 2030, data protection must be a national security priority.

The weaponization of surveillance tools

Authoritarian regimes have used surveillance technology on the African continent to spy on the communication devices of the opposition. The escalation has been made possible through foreign interference. In pursuit of their self-interest, countries like Russia, Israel, and China have allowed the misuse of this unregulated technology by authoritarian governments. Such coercive governments have used foreign observation devices to either suppress opposition or target human rights activists. For instance, Huawei's facial recognition cameras have been previously employed in Uganda to track down opposition figures such as Robert Kyagulanyi, widely referred to as Bobi Wine, who was tracked and arrested among his supporters in a concert in Kampala.

Additionally, geopolitical competition has played as a catalyst in the weaponization of surveillance technology. Countries like US, China and Russia implicitly penetrate the sovereignty and security of states using their products, extracting massive amounts of unregulated data. For instance, in 2021, high-level government officials, diplomats and journalists from Uganda and the US had their mobile devices bugged with an Israeli surveillance tool (Pegasus). More recently, Tal Hanan, an Israeli hacker, has been associated with covert involvement in 30 presidential elections, including Kenya's 2022 general elections. Despite such threats, most African governments are still acquiring and using the notorious machinery rather than investing in their own technology. The danger of the suppliers of these tools leveraging their technological expertise to exploit the continent remains real.

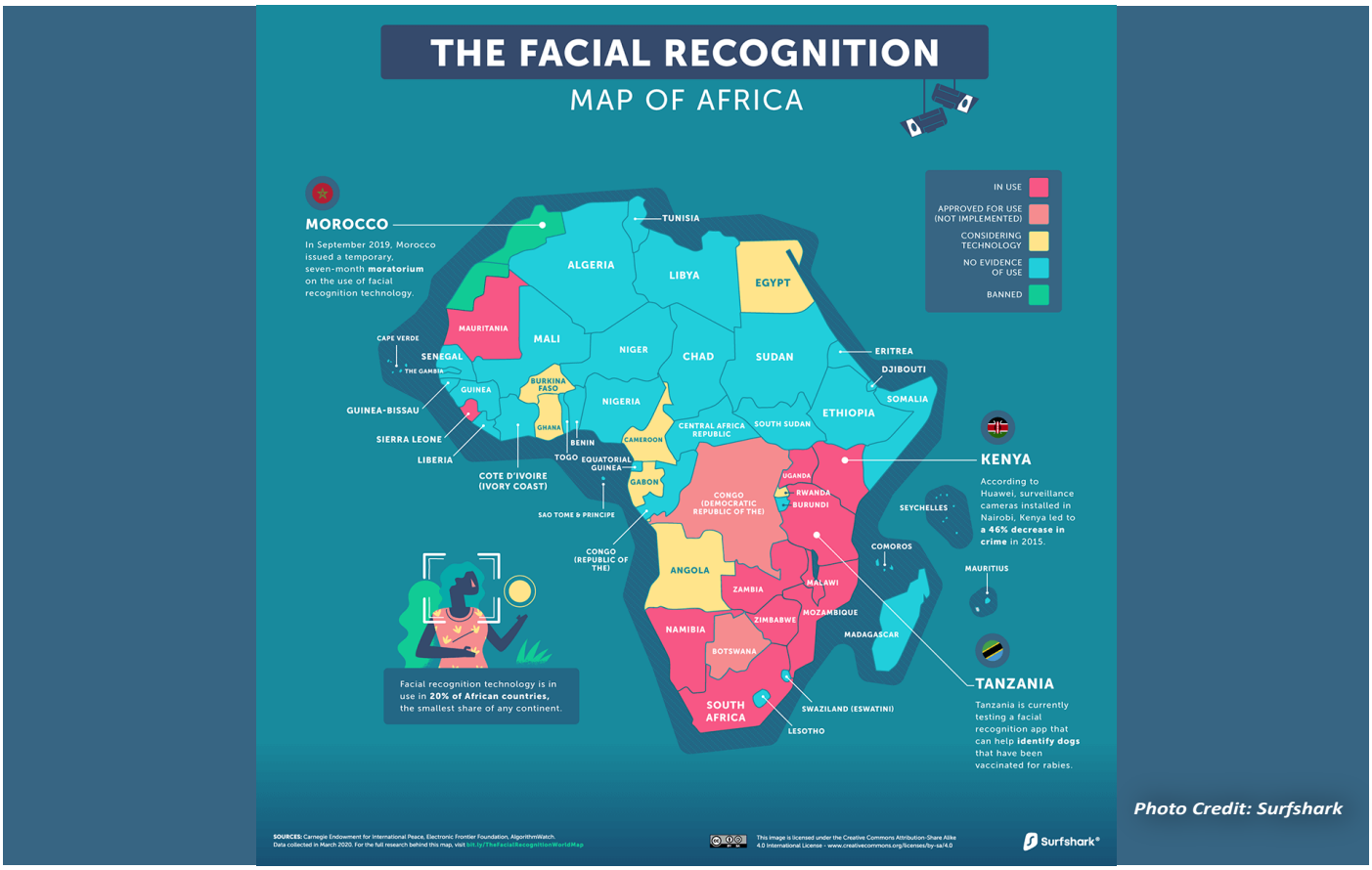


Photo Credit: Surfshark

Rise in digital economic crimes

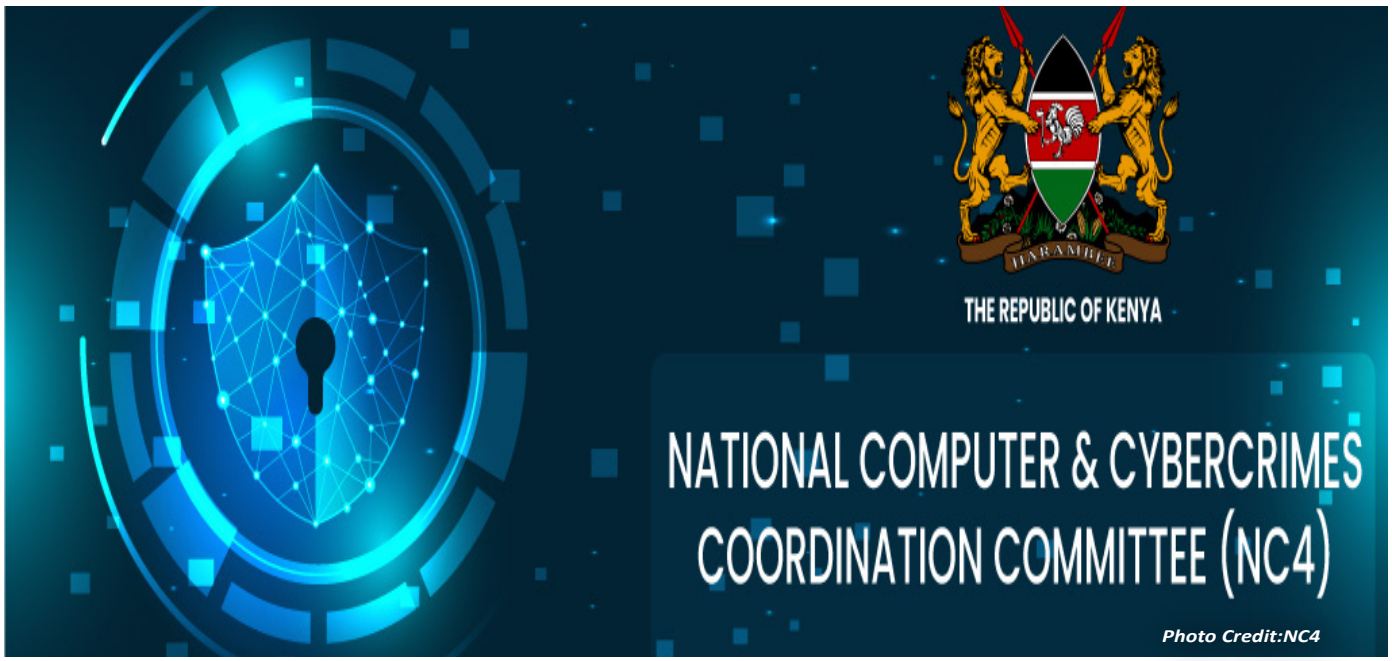
Spyware as a surveillance tool poses a financial threat as it records sensitive data that can threaten a state's national security. The combination of spyware and other malware tools, such as ransomware allows organized criminals and hostile nation-states to obtain and launder illicit profits. Consequently, this may lead to instability of businesses and governments while disrupting supply chains, leaving critical sectors paralyzed. For instance, in 2021, the risk of cybercrimes in Africa amounted to approximately $ 4.1 billion.

Kenya, for instance, has made efforts towards securing its digital economy through the Digital Economy Blue Print, set to be implemented between 2022-2026. The uptake of mobile commerce in the country has resulted in immense economic growth. In 2021, the value of mobile transactions grew by 63.9%, translating to Kes 15.3 trillion. However, the cyberspace vulnerability to possible attacks continues to undermine investments in the digitization of all sectors within the economy. Without adequate safety mechanisms, the digital infrastructure and operations of technological cities such as Konza Technopolis remain vulnerable to foreign criminals.

The risk posed to government data once the digitization of all government services is accessible in one platform is very high. Computer hackers can use advanced surveillance tools to gain unlawful access to sensitive state resources and hold them for ransom. For instance, in Johannesburg, South Africa, hackers demanded a bitcoin ransom in exchange for handing over control of the city's cyber networks. Therefore, the need for African countries to be cautious with foreign surveillance systems cannot be overstated.

Conclusion

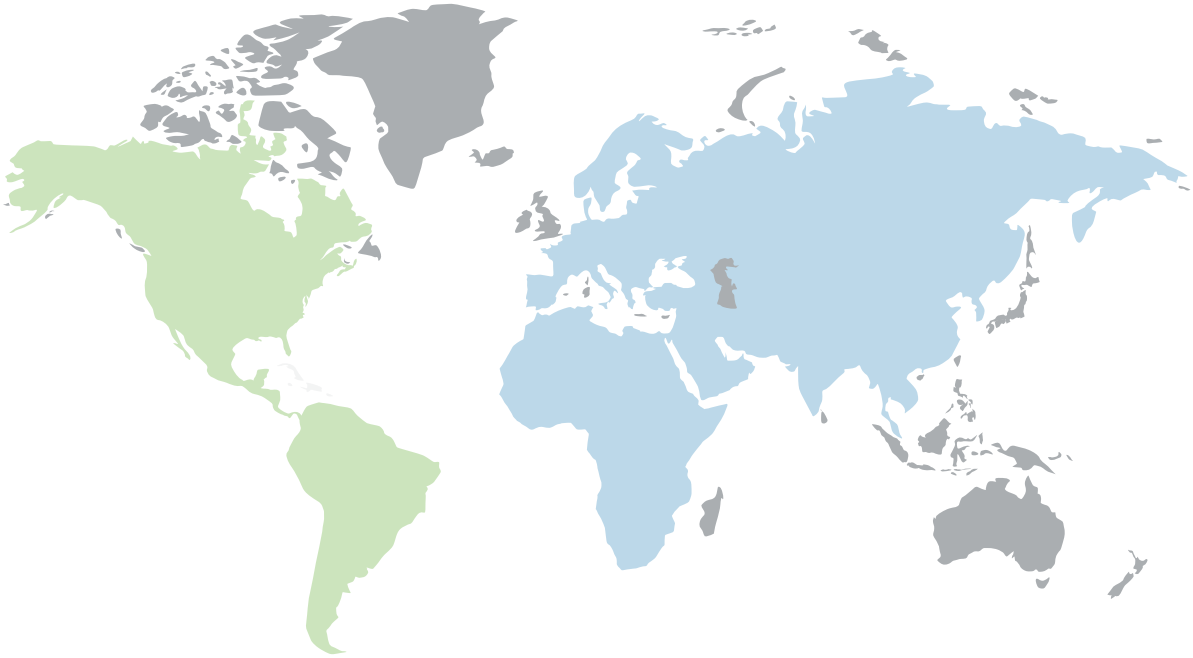
Foreign spyware surveillance technology in Africa warrants effective measures to enhance national security. While the quest is primarily driven by the desire to project power and influence for strategic purposes, the noble intention continues to be undermined by the infringement of data privacy, increased economic crimes and vested interests of political actors. As a regional leader in the technological space, Kenya has the opportunity to drive the continental agenda on inter-regional cooperation to protect Africa's cyberspace.



Recommendations

1. The Ministry of Information, Communication and Digital Economy should;
   a) Strengthen operations of the National Cybercrime Command Centre and the National Computer and Cyber Crimes Coordination Committee (NC4), to regularly update cyber security threats and countermeasures to be included in the national security strategies.
   b) Partner with relevant private sector stakeholders to enhance its public awareness efforts of emerging cyber threats through the National Computer Incident Response Team (N-CRIT) website and on mainstream media.
2. The Ministry of Foreign and Diaspora Affairs should collaborate with the Ministry of Information, Communication and Digital Economy to;
   a) Educate and regularly update Kenyan diplomats and senior government representatives on cyber protection strategies while in foreign duty stations.
   b) Negotiate with country partners, such as the US and Japan, for enhanced technological investments towards implementing the National Digital Economic Blue Print.
   c) Lobby member states of the Africa Union to re-discuss the African Union Convention on Cyber Security and Personal Data Protection with a view to resolve contentious issues inhibiting the harmonization of effective cyber security regulations across the African continent.

The GLOCEPS, Weekly Influential Brief *brings to policy makers precise incisive analyses of policy issues and events locally, regionally and globally. The priority is on topics that have a bearing on Kenya and beyond and are themed on defence and security; diplomacy and foreign policy; governance and ethics; transnational organised crimes; and development. We invite contributions from experts with policy opinions centred on any of the five pillars. Give us your thoughts and feedback through info@gloceps.org*



THE GLOBAL CENTRE FOR POLICY AND STRATEGY
(GLOCEPS)
Research | Knowledge | Influence

Off Kiambu Road, Nairobi Kenya
P.O. Box 27023-00100,Nairobi.
Telephone: 0112401331
Email: info@gloceps.org
Web: www.gloceps.org