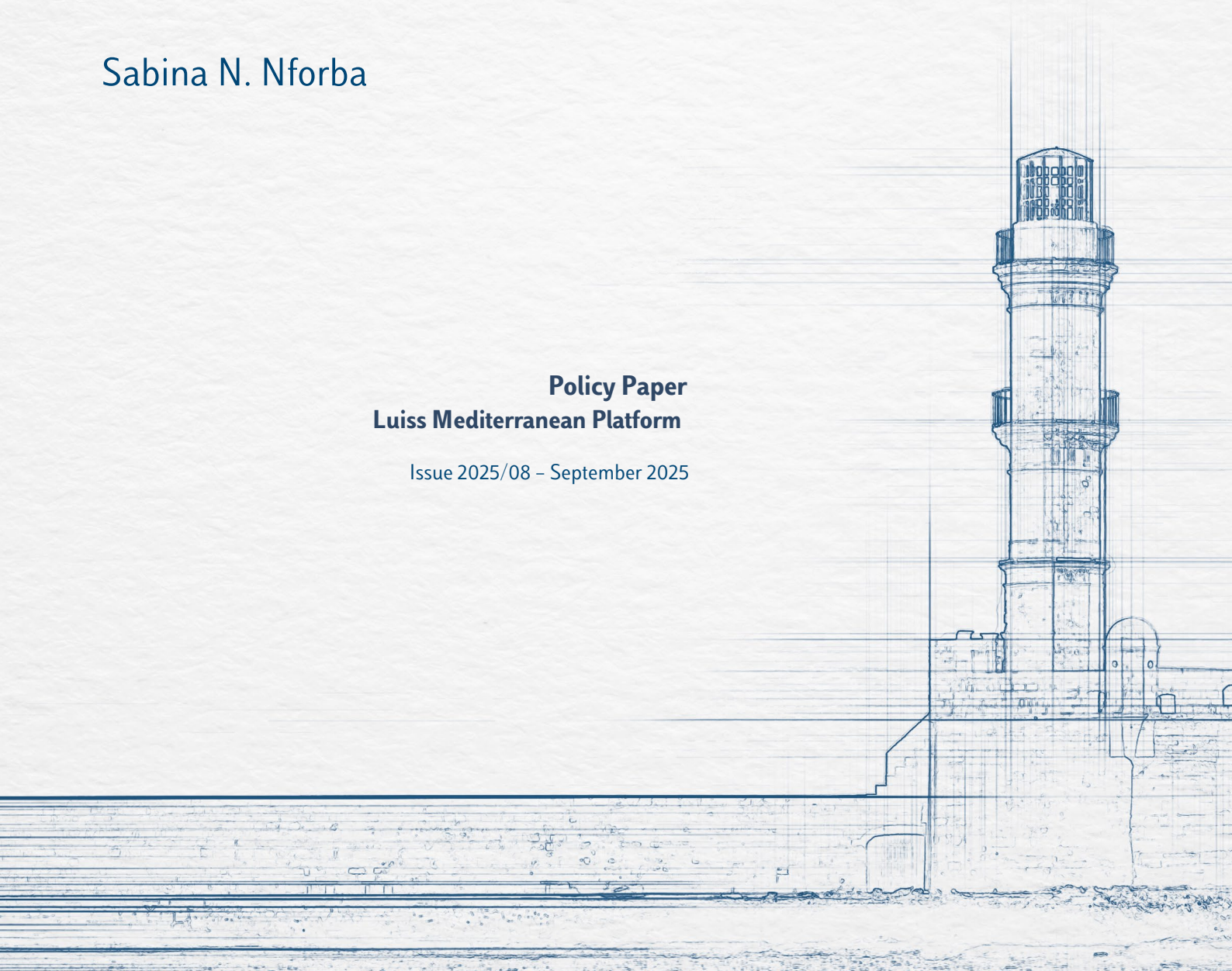
Mediterranean Platform
School of Government

LUISS

The Digital Scramble for Africa: Why Cyber Diplomacy Matters

Sabina N. Nforba



Policy Paper
Luiss Mediterranean Platform

Issue 2025/08 – September 2025

Table of Contents

Executive Summary

This paper examines the effectiveness of current diplomatic measures taken by the African Union and its member states to address growing threats to cybersecurity. Africa has the highest exposure to cyber-attacks per country and continues to be susceptible to aggressors. This analysis shows how existing mechanisms are fragmented and lack incentive for widespread adoption by governments. Given the borderless nature of cyber-attacks, this paper argues that Africa should prioritize cybersecurity and cyber diplomacy in a coordinated, continent-wide approach to safeguard its digital future. These concerns are particularly relevant as the continent embraces new technologies, driven by an expanded youth population. The study concludes by proposing actions such as the enforcement of cyber legislation, reducing dependence on foreign players, investing in education, and training, and promoting public-private sector collaborations to mitigate cyber threats.

Author

Sabina N. Nforba is an interdisciplinary professional with over 8 years of work experience building products and services for value creation through the use of technology in private, public, non-governmental, and international organizations. Areas of focus include technology, innovation, policy, and project management, with a proven track record across a wide geographical span after working in Africa, America, and Europe.

She is currently a Senior Policy Officer at the African Union Commission. She adds value to the Commission by designing programs that improve the delivery of the African Union's Digital Transformation Strategy and Agenda 2063. Sabina has a Masters in Global Public Diplomacy and Sustainable Development from the Luiss School of Government and a Bachelors in Telecommunications from the University of Buea.

1. Introduction

The role of cyber diplomacy in Africa is increasingly critical as global superpowers and private corporations compete for influence over Africa's digital infrastructure, data, governance, and cybersecurity frameworks. The reliance of many African countries on foreign technology and cybersecurity solutions raises significant risks to digital sovereignty, while data exploitation and the absence of a unified cyber diplomacy framework further compound vulnerabilities. Against this backdrop, cyber diplomacy -the use of diplomatic tools and mindsets needed in resolving, or at least managing, the problems in cyberspace[1] - plays a crucial role in providing countries with the set of rules and norms needed to navigate the digital landscape and safeguard their interests in a fast-evolving geopolitical context.

A crucial yet overlooked truth is that cyberspace, despite being a highly technical domain, is ultimately a human construct—designed, governed, and shaped by people. While most countermeasures against cyber-attacks focus on technical solutions, such as strengthening computer networks to defend against and respond to threats, these efforts should be complemented by non-technical approaches that address the human factor. This is where cyber diplomacy becomes essential. Moreover, Africa finds itself entangled in geopolitical rivalries, amplifying the importance of cyber diplomacy in managing the challenges that arise in cyberspace.

This paper evaluates the effectiveness and role of cybersecurity measures implemented in Africa through cyber diplomacy, in the context of superpowers vying for influence in Africa's digital landscape. It begins by outlining the scale of the threats that affect African nations, emphasizing the importance of prioritizing cyber diplomacy. It then explores both internal and external challenges the continent faces in addressing cybersecurity threats, particularly the role of external geopolitical superpowers in influencing African policies, and the implications of their dominance in Africa's cyber domain. Finally, it provides solutions to strengthen Africa's cyber security posture to efficiently manage international relations in its new "borderless" norm.

[1] Shaun Riordan, *Cyberdiplomacy: Managing Security and Governance Online* (Wiley, 2019).

2. The scale of cyber threats in Africa

As Africa rapidly adopted technology, the continent saw its internet penetration rate rise from 9.6% in 2010 to 33% in 2021.[2] While this growth has unlocked significant opportunities, it has also heightened the continent's exposure to cyber threats. Cyber-attacks targeting African states have been diverse in scope, impacting government agencies, financial institutions, critical infrastructure, and electoral commissions, often with devastating effects. The Global Threat Index for June 2024 highlights that Africa experienced the highest volume of attacks, with organizations experiencing about 2,960 cyber-attacks weekly. Ethiopia ranked second globally and first in Africa, underscoring the continent's heightened vulnerability to cyber threats.[3]

This vulnerability is not just a statistical concern—it has played out in real-world incidents that have targeted national security and critical infrastructure. Just a few examples: In June 2020 numerous Ethiopian government websites were hacked to create a multi-faceted pressure on Ethiopia to target and create difficulties in its operation of the Grand Ethiopian Renaissance Dam[4]. This was later attributed to an Egyptian-based hacking group. South Africa experienced a major cyber-attack in July 2019 on its electricity utility[5] while Ghana reported a series of cyber-attacks on its IT systems ahead of elections in 2020[6].

While technical solutions are fundamental in reducing vulnerability against cyber threats, actively using diplomacy as a tool to reduce such cyber risks remains essential, advocating for a more holistic approach that leverages the full range of tools available. In fact, cyber threats frequently stem from geopolitical tensions between state and non-state entities, that present themselves in the form of cross-border actors targeting critical state infrastructure. Diplomacy is therefore essential for promoting international cooperation. Through diplomatic channels, countries can negotiate agreements on cyber norms and approach cyber security from a unified front.

3. Current State of Cyber Diplomacy in Africa

The current state of cyber diplomacy in Africa has evolved over the last few years. Though it has progressed at a very slow pace, there have been several initiatives and instruments that aim to tackle cyber threats. Of key significance is the African Union (AU) Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention[7], which came into force in June 2023. The Convention provides a framework for guaranteeing cyber security in Africa through regulating electronic transactions, protecting personal data, and policing cybercrime. As a continental instrument, the Malabo Convention creates a uniform cyber governance system, ensures unified regulatory approaches between the African Union Member States, and promotes cyber

[2] ITU, "Measuring Digital Development – Facts and Figures 2021," Development Sector Report, 2021.
[3] Check Point , "Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks," July 16, 2024.
[4] Borkena, "Egypt based hackers attempted cyber-attacks on Ethiopian gov't sites," June 22, 2020.
[5] Admire Moyo, "City of Joburg Hit by Cyber Attack," *ITWeb*, October 25, 2019.
[6] Public Services Commission (Ghana), "Ghana faces cyberattack threat ahead of December elections," 2024.
[7] African Union, "African Union Convention on Cyber Security and Personal Data Protection," June 27, 2014.

resilience in the region. However, its implementation has been slow, with only 15 out of 55 African Union member states having signed and ratified it.

At the regional level, the Economic Community of West African States (ECOWAS) and the Southern Africa Development Communities (SADC) have adopted the Directive on Fighting Cybercrime and the Model Law on Computer Crime and Cybercrime, respectively, that obliges member states to establish national cybersecurity strategies and offers guidance for enacting national laws on cybersecurity. In total, 39 nations in Africa have legislations that explicitly address cybercrime as part of their Internet governance frameworks.[8]

Another notable addition is the African Common Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace (CAP), recently adopted by the African Union Peace and Security Council in January 2024 and endorsed by the Assembly of the African Union in February 2024.[9]

This stance held by the AU implies that any low-intensity cyber operation that involves non-consensually penetrating a computer system located on another state's territory violates the target state's sovereignty.[10] With most African countries having relatively weak cyber defense systems compared to the rest of the world, the CAP prohibits more powerful states from engaging in extraterritorial cyber-espionage. The CAP is the most significant document when it comes to the application of international laws in cyberspace in Africa.

Regarding international frameworks, only 5 African countries have signed The Convention on Cybercrime, also known as The Budapest Convention.[11] It is the first international treaty aimed at harmonizing national laws to address internet and computer crime and increase coordination between nations.

While these frameworks reflect Africa's recognition of the importance of cyber diplomacy, their slow adoption and uneven enforcement leave the continent exposed. This limited progress has two major consequences. Externally, Africa becomes vulnerable to the influence of powerful global actors who seek to shape its digital governance according to their own strategic interests (section III). Internally, the gap between formal commitments and practical implementation creates weak points in governance and security systems, undermining democratic integrity and resilience (section IV).

[8] UN Trade and Development, "Cybercrime Legislation Worldwide," accessed September 2025.
[9] African Union, "African Common Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace," 2022.
[10] Kevin Heller, "The African Union (Rightly) Endorses Pure Sovereignty in Cyberspace," February 5, 2024.
[11] Council Of Europe, "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols," accessed September 2025.

4. The external challenge: Africa as a playground for digital geopolitics

The role of external geopolitical players in Africa's digital and cyber security landscape is very relevant. There seems to be an increasing appetite for Africa's digital potential, primarily because of the continent's population of over 1 billion people, particularly its expanding youth, who present substantial amounts of untapped market for digital services, investments, and testing of new technologies.

However, due to the lack of robust Internet governance mechanisms in most African countries, compounded with its weak digital and cyber defense infrastructure, global superpowers exploit these gaps by offering digital solutions and influencing policies that secure their strategic interests. This makes Africa a playground for major competing superpowers, each seeking to have a slice of the pie. To navigate this complex geopolitical landscape, this paper investigates three of these global powers and the influence they exert in Africa - China, Russia, and The West. The Global Economic Governance Forum suggests that in the realm of cyber diplomacy, Africa is aligning with China and Russia.[12] This can be seen through the adoption of digital sovereignty approaches by most African countries, the role of Russia during the negotiations of the UN Cybercrime Convention[13] and the reliance of African countries on technology from these two countries.

4.1. China

As of 2024, 52 African countries and the African Union Commission have signed agreements with China under its Belt and Road Initiative (BRI), which significantly impacted Africa's digital transformation, investing up to 1.8 billion USD through its Digital Silk Road initiative[14]. Key areas of investment are telecommunications, smart cities, e-commerce, and digital payment platforms. In particular, Chinese telecommunication giants have led the rollout of 5G deployment in Africa, signing deals with countries like South Africa, Kenya, and Nigeria, significantly improving infrastructure benefits, as well as increasing job creation and skill development.

Yet, this growing involvement also raises strategic concerns about over-dependence on external actors who retain control over critical information infrastructure. In Kenya, for instance, China was appointed as the lead advisor for the country's national ICT master plan, granting it a central role in shaping Kenya's digital future. In Angola, the Chinese artificial intelligence firm Percent Corporation developed an advanced system for data visualization and analysis to support government decision-making. These examples illustrate how Chinese influence in digital development is not limited to infrastructure—it increasingly extends into the realm of governance and strategic autonomy.[15]

[12] Nnenna Ifeanyi-Ajufo, "The current state of cybersecurity in Africa is the tendency towards a cyber-militarisation approach," Global Economic Governance Forum, n.d.
[13] United Nations, "Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes," n.d.
[14] Dipanjan Roy, "China reportedly investing $ 8.43 bn in Africa as part of Digital Silk Road initiative," *The Economic Times*, October 15, 2021.

[15] Willem Gravett, "Digital neo-colonialism: The Chinese model of internet sovereignty in Africa," *African Human Rights Journal* 20(1), 2020.

China's close ties with many African governments have enabled the diffusion of its concept of 'Internet sovereignty,' which is increasingly shaping how African states approach digital governance. As Beijing refines its domestic model of online censorship and exports a vision of strict state control over digital content, its authoritarian approach resonates with several African regimes that have adopted similar measures. For example, in 2017, the Government of Cameroon shut down internet access in the country's English-speaking regions for 230 days in an effort to suppress dissent and control public discourse.[16]

This ideology of border control over online content has serious consequences for how internet governance and cybersecurity are understood in the region. African government institutions, which often lack the skills, capacities, and resources to effectively implement cyber policies and enforcement measures, may perpetuate cyber discordance - misalignment in digital spaces caused by differences in regulations and policies - rather than enhance cybersecurity.

In summary, over-reliance on China has increased Africa's vulnerability in cyberspace[17]

4.2. Russia

While China aims to expand its geopolitical footprint on Africa's digital domain through heavy investments in digital infrastructure - particularly in countries that have economic hubs or growth potential-, Russia's strategy leverages the cyber domain for enhanced military support, disinformation campaigns, and political manipulation, targeting especially conflict-affected states that are more vulnerable to Russian influence. This approach appears in the 2010 Russian Military Doctrine of the Russian Federation. The doctrine emphasizes that a defining feature of modern conflicts is "the prior implementation of measures of information warfare to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force".[18] In other words, cyberspace is regarded as a medium for the state to dominate the information landscape.[19] This demonstrates Russia's modus operandi in cyberspace, leveraging the rapid and widespread nature of social media in Africa for disinformation, consequently leading to the manipulation of public opinion, disruption of democratic processes, and the creation of social divisions, all of which is instrumental in strengthening Russian influence.

Russia's disinformation campaigns are often anti-democratic, anti-UN, and anti-West, promoting the idea that Western colonies are neo-colonial powers with exploitative intentions, thus shifting public opinion from Western allies to closer alignment with Russia.

Taking the cue from Russia, disinformation campaigns have been on the rise in Africa's domestic political landscape. Research revealed that disinformation campaigns in these countries were connected to domestic governments or political parties with various objectives.[20]

[16] Yano Ritzen, "Cameroon internet shutdowns cost Anglophones millions," *Aljazeera*, January 26, 2018.
[17] Nanjira Sambuli, "Africa is a strategic techno-geopolitical theatre. Will the continent's leaders take advantage of this?" Africa Policy Research Institute, June 9, 2022.
[18] Carnegie Endowment for International Peace, "The Military Doctrine of the Russian Federation," February 9, 2010,
[19] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA, March 2017.
[20] Africa Center For Strategic Studies, "Domestic Disinformation on the Rise in Africa," October 2021.

4.3. The West

Although the USA and Europe have key differences in their strategies, priorities, and methods of engagement with Africa, they are united by a core commitment to an open, free, and secure Internet that respects human rights and freedoms, and aligns with democratic principles. This differs starkly from the internet sovereignty strategies employed by China and Russia and therefore presents a different approach to Africa's digital transformation and cybersecurity. The free internet nations, essentially the US and its allies, seek to maintain the Internet as it is: global and largely free from government interference. They advocate for a multi-stakeholder model, which includes states, the private sector, civil society, and other stakeholders.[21]

This vision is reflected in their actions. Recognizing that a secure and open digital space requires skilled professionals and resilient institutions, both the U.S. and Europe have invested in capacity-building programs to enhance cybersecurity skills and knowledge in Africa. These efforts include training government officials, law enforcement personnel, and cybersecurity professionals through initiatives like the U.S. Cybersecurity Capacity Building Program (CCBP), the EU's Cyber Resilience for Development (Cyber4Dev), and the Africa Cyber Programme (ACP) of the UK Foreign Commonwealth and Development Office.

These differing approaches - China and Russia on one hand, the West on the other hand - reflect broader geopolitical interests and have significant implications for the future of cybersecurity and digital governance in Africa. Indeed, this divergence is shaping a fragmented cybersecurity landscape in Africa, with implications for cross-border data flows, cyber threat response, and digital sovereignty. There is a need for African governments to maintain agency in relationships with different actors to navigate this complex digital ecosystem in a way that is both secure and conducive to economic and social development.

5. The internal challenge: weak cyber diplomacy and cybersecurity in Africa

As Africa undergoes rapid digital transformation, the expansion of digital infrastructure and increased connectivity are reshaping political, economic, and security landscapes. While these advancements present opportunities for innovation, economic growth, and improved governance, they also introduce significant vulnerabilities. Weak cybersecurity frameworks and the absence of coordinated cyber diplomacy expose African nations to internal risks that undermine governance, security, and stability. Two major concerns stand out: the erosion of democratic integrity and the increasing susceptibility to hybrid warfare.

The expansion of digital infrastructure has reshaped governance and political engagement across Africa, but in the absence of strong cybersecurity mechanisms, it is also being exploited to weaken democratic institutions. Some African governments are using digital technologies for mass surveillance of political opponents and activists, targeted monitoring of users' digital footprints, and internet shutdowns to suppress dissent. These

[21] Riordan, *Cyberdiplomacy: Managing Security and Governance Online.*

actions reinforce authoritarian models of cyber governance, further deteriorating already fragile democratic systems.[22]

Weak cybersecurity mechanisms also allow for the proliferation of disinformation and misinformation campaigns, especially during elections. A prominent example occurred during the 2017 Kenyan elections, when Cambridge Analytica[23] used private data from Kenyan citizens for a micro-targeting campaign that fueled ethnic tensions and fear. Manipulative political messaging on social media influenced voter perceptions, demonstrating how digital tools can be weaponized to distort democratic processes.

Additionally, election integrity in Africa continues to be undermined by the fact that electoral infrastructure remains highly vulnerable to cyber threats, with electoral systems and databases susceptible to hacking and manipulation through cyber-attack. For instance, during Nigeria's 2019 elections, reports of a cyber-attack on the Independent National Electoral Commission (INEC), raised concerns about the security of digital voting platforms. Although INEC claimed that its system was secure, the incident underscored growing risks of electoral interference through cyber means.[24] Ultimately, without stronger digital security frameworks, electoral integrity will continue to be at risk, eroding public trust, undermining democracy, and leading to political instability.

The increasing integration of digital technologies into governance, diplomacy, and national security also makes Africa more exposed to hybrid warfare—a strategy that blends cyber operations with conventional conflict tactics to achieve strategic objectives. Both state and non-state actors are using cyber tools to disrupt adversaries, manipulate negotiations, and exert influence over geopolitical disputes. A notable example of cyber-enabled conflict occurred during negotiations over the Grand Renaissance Dam, when the Egypt-based group Cyber Horus claimed responsibility for an attack to interrupt negotiations that were underway between the Ethiopian and Egyptian governments on a 4.6-billion-dollar dam that was being built by Ethiopia over the Blue Nile.[25]

6. A call to action

Africa finds itself at the center of a new era of geopolitical competition—one increasingly defined by data, connectivity, and influence. As shown in this Brief, in the face of mounting digital challenges from both external and internal sources, cyber diplomacy remains a critical tool for navigating this complex terrain. It offers African states the means to assert digital sovereignty, build strategic alliances, and shape the rules of engagement in cyberspace. In this context, a bold and coordinated call for action is imperative to ensure Africa's interests are protected and its digital future is forged on its own terms. Against this backdrop, four priority actions stand out as essential steps for Africa to secure its digital future and assert its agency in the evolving cyber domain:

- **Establish an enforcement mechanism to adopt and implement cybersecurity legislation:** The AU should prioritize cybersecurity by working collaboratively to establish enforcement mechanisms that encourage the adoption and implementation of regional and international instruments like the

[22] Tony Roberts et al., "Surveillance Law in Africa: a review of six countries," Research Report, Institute of Development Studies (IDS), 2021.
[23] Justina Crabtree, "Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections," *CNBC*, March 2018.
[24] Godson Bill, "Safeguarding democracy: Cybersecurity threats to elections in Africa," *GhanaWeb*, July 2024.
[25] Zecharias Zelelem, "An Egyptian Cyber-attack on Ethiopia by Hackers is the latest strike over the Grand Dam," *QUARTZ*, July 21, 2022.

Malabo and Budapest Conventions. Furthermore, these frameworks need implementation guidelines to ensure the groundwork be laid for uniformity in their application. This would create a harmonized system for dealing with cyber threats not only across the continent, but globally.

- **Reduce dependence on external players:**
  To preserve its sovereignty in the cyber domain, Africa should reduce its dependence on external players for critical infrastructure and instead invest in its own infrastructure. Critical means of this investment includes encouraging local tech entrepreneurship and innovation, such as Andela, Flutterwave and Jumia. This way. African nations can balance their autonomy with the ways to benefit from the great power competition, to keep the continent and individual countries' interests first.

- **Education and training for diplomats and cybersecurity professionals:**
  As the cyber domain has become critical in international relations, national security, and economic development, it is vital to equip diplomats with the necessary skills to understand cyber policies, negotiate cyber agreements and treaties, and advocate for human rights and ethical cyber practices. There is also a need to match technical cybersecurity demands with cybersecurity professionals who are trained in updated practices to safeguard critical infrastructure.

- **Promote public-private sector partnerships and foster multilateralism:**
  The AU and member states should engage more actively in multilateral and public-private partnership efforts aimed at enhancing cybersecurity. Governments need to foster cooperation with technology companies, cybersecurity firms, and research institutions to facilitate information-sharing on cyber threats and jointly develop strategies that bolster cyber resilience.

7. Conclusion

The AU and its member states have recognized the importance of cybersecurity and expressed a growing commitment to address the escalating threats emerging from cyberspace. However, as outlined above, the existing mechanisms remain weak and ill-equipped to respond to the complex and evolving nature of contemporary cyber threats. To strengthen its cybersecurity standing, Africa should prioritize cyber diplomacy by establishing effective enforcement mechanisms for cybersecurity legislation, reducing over-reliance on global superpowers, investing in the training of cyber diplomats and technical experts, and promoting multilateral cooperation and strategic public-private partnerships. These steps are essential to safeguarding the continent's digital future and ensuring the security and sovereignty of its cyberspace.

These goals and initiatives should be supported by other countries that share the vision for an open, secure, and resilient cyberspace. Italy, as one of these countries, can contribute to this effort through its Mattei plan for Africa which emphasizes energy, infrastructure, and digital corporations. Within this framework, Italy can encourage investments in Africa-led cybersecurity solutions to reduce dependence on foreign actors, enhance collaboration between Italian and African law enforcement agencies to counter cybercrime, and establish cybersecurity training programs for African policymakers, law enforcement, and IT professionals.

Mediterranean Platform
School of Government

LUISS

Mediterranean Platform

Founded in 2022, and directed by Prof. Luigi Narbone, the Mediterranean Platform is a research, dialogue, and educational programme at the School of Government, Luiss Guido Carli. It offers a space for collective reflection on the opportunities and challenges of the Mediterranean region and promotes informed policymaking and advocacy at the national and transnational levels.

mp.luiss.it

School of Government, Luiss Guido Carli

Luiss School of Government SoG is a graduate school training high-level public and private officials to handle political and government decision-making processes. Founded in 2010, SoG has become one of the most relevant institutions in Europe for teaching and research. As part of Luiss University is now ranked among the top 15 in the world (and 1st in Italy) for Politics and International Studies according to the QS World University Rankings by Subject 2023.

sog.luiss.it

Published by:
Luiss Guido Carli - Viale Pola 12, 00198 Rome, Italy
sog.luiss.it