

Artificial Intelligence, Cyber Resilience and Digital Sovereignty: Securing Africa's Digital Transformation in an Evolving Geopolitical Order

Dr. Alexander Odartey Lamptey

African Peace Support Trainers Association-APSTA, Greater Accra, Ghana

ABSTRACT

Rapid advances in mobile technologies, digital financial services, cloud computing, artificial intelligence (AI), big data analytics, and digital public infrastructure are creating unprecedented opportunities for economic growth, innovation, inclusion, and regional integration. The African Union (AU) recognizes digital transformation as a critical enabler of Agenda 2063 and has adopted several continental frameworks, including the Digital Transformation Strategy for Africa (2020–2030), to guide this transition (African Union, 2020). Notwithstanding these opportunities, Africa's digital transformation is unfolding within a progressively volatile geopolitical environment characterized by technological competition, cyber insecurity, and growing concerns regarding digital dependence. Cybercrime, dark web hacking, ransom ware attacks, cyber espionage, digital disinformation campaigns, and attacks on critical national infrastructure are becoming sophisticated and costly daily. According to the International Telecommunication Union (2024), many African countries continue to face significant cyber security readiness gaps despite growing digital connectivity. These vulnerabilities threaten not only economic development but also state sovereignty, institutional legitimacy, and regional stability. Simultaneously, global competition over emerging technologies, artificial intelligence, semiconductor production, data governance, and digital infrastructure is transforming international relations. Digital technologies have become strategic assets that influence economic competitiveness, national security, and geopolitical influence. In this context, digital sovereignty has emerged as an essential component of economic sovereignty and strategic autonomy. Digital sovereignty refers to the capacity of states and societies to exercise meaningful control over digital infrastructure, data resources, technological innovation, and governance frameworks. This paper argues that Africa's pursuit of economic sovereignty and geopolitical relevance requires a deliberate focus on three interconnected pillars: artificial intelligence, cyber resilience, and digital sovereignty. Artificial intelligence presents opportunities to strengthen cyber security through predictive analytics, threat intelligence, automated response systems, and enhanced situational awareness. Cyber resilience enables institutions to anticipate, withstand, recover from, and adapt to cyber disruptions while maintaining critical functions. Digital sovereignty ensures that African countries retain control over strategic digital assets and technological development pathways.

KEYWORDS

Artificial Intelligence, Cyber Resilience, Digital Sovereignty, Cyber security Governance, Africa

I. KEY POINTS

The paper settles that, by investing in AI governance, advanced cyber security capabilities, sovereign digital infrastructure, and regional cooperation mechanisms, African states can strengthen both digital control and broader economic sovereignty while contributing to peace, security, and sustainable development. The following five key points are crucial:

- Digital transformation presents significant opportunities for economic growth, inclusion, and innovation but simultaneously increases exposure to cyber threats and technological dependencies.
- Digital sovereignty has become a strategic component of economic sovereignty and requires greater African control over data, digital infrastructure, and emerging technologies.
- Artificial intelligence can significantly enhance cyber resilience through predictive analytics, threat detection, and automated incident response capabilities.
- Weak institutional capacities, fragmented regulatory frameworks, and dependence on foreign technologies continue to undermine Africa's digital security posture.
- Strengthening continental cooperation, investing in indigenous innovation, and building resilient cyber security ecosystems are essential for securing Africa's digital future.

II. BACKGROUND AND INTRODUCTION

Digitalization has become a major determinant of economic competitiveness, governance effectiveness, and national resilience in both developed and developing countries. The global economy is increasingly driven by data, digital technologies, and knowledge-based innovations. Across Africa, governments, businesses, and citizens are embracing digital technologies to improve service delivery, increase financial inclusion, expand market access, and accelerate socio-economic development. The continent has witnessed remarkable growth in digital connectivity over the past decade. Mobile technologies, digital payment systems, e-commerce platforms, digital identity systems, and e-government services are transforming how citizens interact with governments and markets. The expansion of mobile money services in countries such as Kenya, Ghana, Rwanda, and Tanzania demonstrate the transformative potential of digital innovation in promoting inclusive development and economic participation.

Recognizing these opportunities, the African Union has adopted several strategic frameworks designed to support digital transformation and technological advancement. The Digital Transformation Strategy for Africa (2020–2030) envisions a digitally empowered continent that leverages technology to achieve inclusive growth and sustainable development. Complementary frameworks such as the African Union Data Policy Framework (2022) and the Continental Artificial Intelligence Strategy (2024) further underscore the continent's commitment to building a resilient digital future.

However, digital transformation is occurring within an increasingly contested geopolitical environment. Competition among major powers for influence over digital infrastructure, artificial intelligence, semiconductor technologies, data governance standards, and cloud computing services is reshaping global power relations. Control over digital ecosystems has become a critical source of economic leverage and strategic influence, prompting growing concerns regarding technological dependency and digital sovereignty. For African countries, this evolving environment presents both opportunities and risks. While external investments and technology transfers can accelerate digital development, excessive dependence on foreign technologies may undermine strategic autonomy and limit domestic innovation capacities. Furthermore, increased digital connectivity has expanded the attack surface for cybercriminals, hostile actors, and transnational threat networks.

Cyber security has therefore emerged as a critical component of national security, economic resilience, and sustainable development. Recent cyber-attacks targeting financial institutions, telecommunications networks, healthcare systems, and government agencies demonstrate the increasing vulnerability of digital infrastructure across the continent. The growing sophistication of cyber threats requires a shift from reactive cyber security approaches toward more comprehensive cyber resilience strategies capable of managing uncertainty and disruption. Against these backdrops, artificial intelligence, cyber resilience, and digital sovereignty have become increasingly interconnected concepts within Africa's emerging security architecture. Together, they provide a framework for understanding how African states can secure digital transformation while advancing broader objectives relating to economic sovereignty, geopolitical relevance, and sustainable peace.

1. Digital Transformation and Geopolitical Competition

Africa's digital transformation agenda is unfolding during a period in which digital technologies have become central to economic growth, governance innovation, and strategic competition. Governments across the continent are investing heavily in broadband infrastructure, digital public services, fintech ecosystems, smart governance initiatives, and emerging technologies such as artificial intelligence and cloud computing (World Bank, 2024). The rapid growth of digital ecosystems has generated significant developmental benefits. Digital financial services have expanded access to banking and credit, particularly among previously underserved populations. E-government platforms have improved transparency and service delivery, while digital entrepreneurship has created new economic opportunities for youth and small businesses.

Yet digital expansion has also introduced new vulnerabilities. Cybercrime has become one of the fastest-growing threats to Africa's digital economy. Financial fraud, ransom ware attacks, phishing schemes, identity theft, and cyber espionage are increasingly targeting both public and private institutions. The World Economic Forum (2024) notes that cyber threats continue to evolve in sophistication, exploiting institutional weaknesses and technological gaps across both developed and developing economies. Several structural factors contribute to Africa's cyber vulnerability. Many countries continue to face shortages of cyber security professionals, weak regulatory frameworks, insufficient investment in cyber infrastructure, and fragmented incident response mechanisms. These challenges are compounded by increasing dependence on foreign technology providers and externally controlled digital infrastructure.

At the same time, geopolitical competition over emerging technologies is intensifying. Artificial intelligence, quantum computing, semiconductor production, cloud infrastructure, and data governance are increasingly viewed as strategic assets that shape national power and influence (Nye, 2017). Major Powers are investing heavily in these technologies while competing to establish international standards and governance frameworks. The intersection of digital transformation, cyber insecurity, and geopolitical competition therefore necessitates a comprehensive approach that integrates cyber security, governance, technological innovation, and institutional resilience.

2. *Artificial Intelligence, Cyber Resilience and Digital Sovereignty*

Artificial intelligence (AI) is rapidly transforming the global technological landscape and is increasingly recognized as a strategic enabler of economic development, governance innovation, and national security. The ability of AI systems to process vast amounts of data, identify patterns, generate predictive insights, and automate decision-making processes has profound implications for how governments, businesses, and security institutions operate. For Africa, AI presents a unique opportunity to accelerate development while simultaneously addressing longstanding governance and security challenges. AI-powered solutions are already being deployed in agriculture, healthcare, financial services, education, and public administration across several African countries. These innovations demonstrate the potential of AI to improve service delivery, enhance productivity, and promote inclusive growth.

However, the strategic significance of AI extends beyond economic development. Increasingly, AI is becoming a critical component of cyber security and digital resilience. Traditional cyber security approaches are often reactive and heavily dependent on human intervention. The growing complexity and speed of cyber threats make it increasingly difficult for conventional systems to identify and respond effectively to attacks. AI-enabled cyber security solutions address this challenge by enhancing threat detection, anomaly identification, predictive analytics, and automated response capabilities (Kott et al., 2022).

The application of AI to cyber security is particularly relevant in Africa, where many institutions face resource constraints, limited technical expertise, and insufficient cyber security infrastructure. AI can help bridge these capacity gaps by automating routine tasks, improving efficiency, and enabling faster responses to cyber incidents. By augmenting human capabilities, AI can significantly strengthen cyber resilience across both public and private sectors. Cyber resilience refers to the ability of systems, organizations, and societies to anticipate, withstand, recover from, and adapt to cyber disruptions while maintaining essential functions. Unlike traditional cyber security approaches that focus primarily on prevention, cyber resilience emphasizes adaptability, continuity, and recovery. It recognizes that cyber incidents are inevitable and therefore prioritizes preparedness and institutional learning.

This distinction is particularly important in the African context. Given the increasing sophistication of cyber threats and the uneven distribution of cyber security capabilities across the continent, complete prevention of cyber incidents is unrealistic. Instead, governments and institutions must develop resilience strategies that enable them to absorb shocks and continue operating during periods of disruption. Such strategies require

investments in governance systems, incident response capabilities, workforce development, risk management, and technological innovation.

Digital sovereignty has emerged as a response to these concerns. While definitions vary, digital sovereignty generally refers to the ability of states and societies to exercise meaningful control over digital infrastructure, data resources, technological development, and digital governance frameworks. It is increasingly viewed as a prerequisite for economic sovereignty and strategic autonomy in the digital age. For African countries, digital sovereignty involves several interconnected dimensions.

- It requires greater control over data generated within national borders. Data has become a critical economic and strategic asset, often described as the "new oil" of the digital economy. Yet much of Africa's data is collected, processed, stored, and monetized by foreign entities, limiting opportunities for local value creation and innovation.
- Digital sovereignty requires investment in indigenous technological capabilities. Dependence on imported technologies and externally controlled digital infrastructure creates vulnerabilities that can undermine both economic resilience and national security. Strengthening domestic innovation ecosystems is therefore essential for reducing technological dependency.
- Digital sovereignty requires effective governance frameworks capable of regulating emerging technologies while protecting citizens' rights and promoting innovation. Regulatory capacity remains uneven across the continent, highlighting the need for coordinated policy development and institutional strengthening.

Ultimately, the convergence of AI, cyber resilience, and digital sovereignty presents both opportunities and challenges for Africa. Harnessing the benefits of AI while reducing technological dependency requires deliberate investments in institutions, infrastructure, governance, and human capital. Success will depend on the ability of African states and regional organizations to develop coherent strategies that balance innovation, security, and sovereignty objectives.

3. *Strengthening African Institutions and Capabilities for Digital Sovereignty*

The realization of digital sovereignty and cyber resilience in Africa depends fundamentally on the strength and effectiveness of African institutions. While technological innovation is essential, technology alone cannot guarantee resilience or sovereignty. Strong governance structures, capable institutions, coordinated policies, and skilled human resources are equally important.

4. *The Role of the African Union*

The African Union occupies a central position in shaping the continent's digital future. Through initiatives such as the Malabo Convention, the Digital Transformation Strategy for Africa, the Data Policy Framework, and the Continental Artificial Intelligence Strategy, the AU has established a comprehensive policy architecture for digital governance (African Union, 2014, 2020, 2022, and 2024). These frameworks provide a common vision for digital transformation, cyber security governance, and technological development. However, implementation remains uneven across member states. Many countries have yet to fully domesticate or operationalize key continental instruments, limiting their effectiveness. To

address this challenge, the AU should strengthen implementation support mechanisms, enhance monitoring and evaluation systems, and facilitate knowledge-sharing among member states. A continental African Cyber Resilience and Digital Sovereignty Centre could provide a strategic platform for coordinating cyber security research, incident response cooperation, policy development, and AI governance initiatives. Such an institution would strengthen continental preparedness while reducing duplication of efforts across member states.

5. *Regional Economic Communities as Strategic Enablers*

Regional Economic Communities (RECs) play a critical role in translating continental objectives into practical regional initiatives. Organizations such as ECOWAS, SADC, EAC, ECCAS, COMESA, and IGAD possess unique advantages in promoting cooperation among neighbouring states and addressing transnational challenges. Cyber threats frequently transcend national borders, making regional cooperation indispensable. Cybercriminal networks exploit jurisdictional gaps, weak regulatory coordination, and disparities in institutional capacity. Regional cooperation can therefore enhance resilience by facilitating information sharing, harmonizing regulations, coordinating responses, and supporting joint capacity-building initiatives. RECs should prioritize the establishment of regional cyber threat intelligence platforms, cyber security training centres, and coordinated incident response mechanisms. Strengthening interoperability among national cyber security institutions would significantly improve regional preparedness and resilience.

6. *National Governments and Cyber security Governance*

National governments remain the primary actors responsible for securing critical infrastructure, protecting citizens, and regulating digital ecosystems. Effective cyber security governance requires comprehensive national strategies that integrate security, development, innovation, and sovereignty objectives. Governments should establish and regularly update national cyber security strategies aligned with continental frameworks. These strategies should clearly define institutional responsibilities, establish incident response protocols, and promote collaboration between government agencies, private sector actors, and civil society organizations. Investment in critical digital infrastructure should be accompanied by corresponding investments in cyber security architecture. Financial systems, telecommunications networks, healthcare institutions, transportation systems, and public administration platforms require robust protection mechanisms capable of withstanding increasingly sophisticated threats. Furthermore, governments should strengthen legal and regulatory frameworks relating to data protection, cyber security, artificial intelligence, and digital governance. Effective regulation is essential for balancing innovation with security, accountability, and citizen protection.

7. *Indigenous Innovation and Technological Capability*

A major obstacle to Africa's pursuit of digital sovereignty is its continued dependence on foreign technologies, digital platforms, cloud infrastructure, and software ecosystems. While international technology partnerships remain important, excessive reliance on external providers creates vulnerabilities relating to data security, strategic autonomy, and economic competitiveness. Building indigenous technological capability is therefore central to achieving sustainable digital sovereignty. African governments, universities, research institutions, and private sector actors must invest in local innovation ecosystems capable of developing home-grown solutions to African challenges. Such investments should focus on

artificial intelligence, cyber security technologies, cloud computing, data analytics, digital public infrastructure, and emerging technologies.

The development of local data centres and sovereign cloud infrastructure can further strengthen digital sovereignty by improving control over strategic digital assets. Investments in local digital infrastructure not only enhance security and resilience but also create opportunities for job creation, technology transfer, and economic diversification (World Bank, 2024). In addition, African universities and research institutions must play a more prominent role in artificial intelligence development. Supporting African-led AI research can help ensure that technological innovation reflects local priorities, values, and socio-economic realities. This approach aligns with growing calls for epistemic sovereignty and locally driven technology governance models.

8. *Public-Private Partnerships and Multi-Stakeholder Collaboration*

The complexity of cyber security challenges requires collaboration among governments, private sector actors, civil society organizations, academic institutions, and international partners. No single stakeholder possesses sufficient resources or expertise to address cyber security risks independently. Public-private partnerships are particularly important because much of Africa's digital infrastructure is owned or operated by private entities. Telecommunications companies, internet service providers, financial institutions, cloud service providers, and technology firms play critical roles in maintaining digital security and resilience. Effective collaboration can facilitate information sharing, joint threat assessments, incident response coordination, and cyber security awareness initiatives. Governments should therefore create enabling environments that encourage cooperation while protecting national security interests and commercial confidentiality.

Civil society organizations also play a crucial role in promoting digital rights, accountability, digital literacy, and citizen participation in technology governance. Their involvement can help ensure that cyber security and digital sovereignty initiatives remain inclusive and aligned with democratic principles. International partners can further contribute through technical assistance, capacity building, and knowledge-sharing programmes. However, such partnerships should be structured in ways that strengthen local ownership and avoid reinforcing dependency relationships. Africa's digital transformation must ultimately be driven by African priorities and interests (United Nations Development Programme [UNDP], 2024).

9. *Human Capital Development and Digital Skills*

Human capital remains one of the most important determinants of cyber resilience and digital sovereignty. Despite significant progress in digital adoption, many African countries continue to experience shortages of cyber security professionals, AI specialists, data scientists, digital policy experts, and technology entrepreneurs. According to recent estimates, the global cyber security workforce gap continues to widen, with developing regions facing particularly acute shortages. Addressing these skills deficits requires comprehensive investments in education, professional training, certification programmes, and lifelong learning opportunities. Governments should work closely with universities, technical institutions, and industry partners to develop curricula that respond to emerging technological trends and labour market demands.

Cyber security, artificial intelligence, data governance, and digital innovation should become integral components of national education strategies. Special emphasis should be placed on

youth and women, whose participation remains essential for achieving inclusive digital transformation. Expanding access to digital education and entrepreneurship opportunities can help address unemployment challenges while simultaneously strengthening Africa's digital economy. Furthermore, strengthening public sector digital competencies is equally important. Government officials responsible for policy development, regulation, and cyber security oversight require continuous training to keep pace with rapidly evolving technological developments.

III. TOWARDS AN AFRICAN DIGITAL SOVEREIGNTY FRAMEWORK

Africa's digital future requires a governance framework that integrates technological innovation, cyber security resilience, economic development, and strategic autonomy. Digital sovereignty should not be interpreted as technological isolation or protectionism. Rather, it should be understood as the ability to participate effectively in the global digital economy while retaining meaningful control over critical digital assets and policy decisions. An African Digital Sovereignty Framework should therefore be built around five interconnected pillars:

- Secure and resilient digital infrastructure.
- Effective cyber security governance and institutions.
- Indigenous technological innovation and research capacity.
- Regional cooperation and policy harmonization.
- Responsible, ethical, and inclusive AI governance.

Together, these pillars can provide the foundation for a resilient digital ecosystem capable of supporting economic sovereignty, peace, security, and sustainable development across the continent.

IV. CONCLUSION

Africa's digital transformation represents one of the most significant opportunities for advancing economic growth, social inclusion, governance effectiveness, and regional integration in the twenty-first century. Digital technologies are reshaping every aspect of economic and political life, creating new opportunities while simultaneously introducing new vulnerabilities. This paper has argued that artificial intelligence, cyber resilience, and digital sovereignty are mutually reinforcing pillars of Africa's emerging security architecture. Artificial intelligence offers significant opportunities to strengthen cyber security capabilities, improve decision-making, and enhance institutional effectiveness. Cyber resilience provides the capacity to anticipate, withstand, recover from, and adapt to increasingly complex cyber threats. Digital sovereignty ensures that technological transformation contributes to strategic autonomy, economic sovereignty, and long-term development objectives.

As geopolitical competition increasingly extends into the digital domain, African states must adopt proactive strategies that strengthen institutions, invest in indigenous technological capabilities, and promote regional cooperation. Failure to do so risks deepening technological dependency and exposing critical systems to external vulnerabilities. The future of Africa's economic sovereignty will depend in part on its ability to govern digital

transformation effectively. By investing in AI governance, cyber security capacity, sovereign digital infrastructure, and human capital development, African countries can build resilient digital ecosystems that support peace, security, innovation, and sustainable development. Such efforts will be essential for ensuring that Africa remains an active and influential participant in the emerging global digital order.

V. POLICY AND STRATEGIC RECOMMENDATIONS

A. For the African Union

- Establish an African Cyber Resilience and Digital Sovereignty Centre to coordinate continental cyber security initiatives and AI governance efforts.
- Accelerate ratification and domestication of the Malabo Convention across all AU member states.
- Develop continent-wide standards on AI governance, cyber security, digital infrastructure protection, and data sovereignty.
- Strengthen implementation mechanisms for the Digital Transformation Strategy for Africa and the Continental Artificial Intelligence Strategy.

B. For Regional Economic Communities

- Create regional cyber threat intelligence-sharing platforms to facilitate early warning and coordinated responses.
- Establish regional cyber security training and capacity-building centres.
- Harmonize cyber security legislation and digital governance frameworks across member states.
- Promote regional cooperation on critical digital infrastructure protection.

C. For National Governments

- Develop and regularly update national cyber security and AI strategies aligned with AU frameworks.
- Invest in sovereign digital infrastructure, including local data centres, cloud services, and secure government digital platforms.
- Strengthen national Computer Emergency Response Teams (CERTs) and cyber security incident response mechanisms.
- Expand digital literacy and cyber security awareness programmes for citizens and public institutions.
- Enhance regulatory frameworks relating to data protection, AI governance, and digital rights.

D. For Academic and Research Institutions

- Expand research programmes in artificial intelligence, cyber security, digital governance, and emerging technologies.
- Strengthen partnerships between universities, governments, and industry to support innovation and technology transfer.

- Promote African-led AI research and innovation ecosystems that address local development and security challenges.

E. For Development Partners and the Private Sector

- Support African-led digital transformation initiatives through equitable partnerships and capacity-building programmes.
- Facilitate technology transfer arrangements that strengthen local ownership and sustainability.
- Promote responsible and ethical AI development consistent with African values and priorities.
- Invest in workforce development initiatives that strengthen cyber security and digital innovation capabilities across the continent.

REFERENCES

- [1] African Union Commission. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).
- [2] African Union Commission. (2020). Digital Transformation Strategy for Africa (2020–2030).
- [3] African Union. (2022). African Union Data Policy Framework. African Union Commission.
- [4] African Union. (2024). Continental Artificial Intelligence Strategy. African Union Commission.
- [5] Castells, M. (2010). The rise of the network society (2nd Ed.). Wiley-Blackwell.
- [6] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cyber resilience: A systematic review. *Risk Analysis*, 42(1), 145–173. <https://doi.org/10.1111/risa.13670>
- [7] Economic Commission for Africa. (2023). Africa digital economy report 2023. United Nations Economic Commission for Africa.
- [8] Effoduh, J. O. (2026). Decolonizing the governance of artificial intelligence in Africa: From normative mimicry to epistemic sovereignty. *Science and Public Policy*, 53(2), 245–257.
- [9] Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 1(1). <https://doi.org/10.1162/99608f92.8cd550d1>
- [10] International Telecommunication Union. (2024). Global cybersecurity index 2024. ITU.
- [11] Jansen, B., Kadenko, N., Broeders, D., van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 101862. <https://doi.org/10.1016/j.giq.2023.101862>
- [12] Kello, L. (2017). The virtual weapon and international order. Yale University Press.
- [13] Kott, A., Golan, M. S., Trump, B. D., & Linkov, I. (2022). Cyber resilience: By design or by intervention? *IEEE Security & Privacy*, 20(2), 32–39.
- [14] Kwet, M. (2019). Digital colonialism: US Empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. <https://doi.org/10.1177/0306396818823172>
- [15] Lewis, J. A. (2021). Cyber security and critical technologies in Africa. Center for Strategic and International Studies.

- [16] Linkov, I., & Kott, A. (2018). Fundamental concepts of cyber resilience: Introduction and overview. In I. Linkov & A. Kott (Eds.), *Cyber resilience of systems and networks* (pp. 1–25). Springer.
- [17] Mueller, M. (2017). *Will the internet fragment? Sovereignty, globalization and cyberspace*. Polity Press.
- [18] Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
- [19] Pawlak, P. (2018). *Riding the digital wave: The impact of cyber capacity building*. European Union Institute for Security Studies.
- [20] United Nations Development Programme. (2024). *Digital development report for Africa*. UNDP.
- [21] World Bank. (2023). *Cyber security capacity building in Africa: Strengthening resilience in the digital age*. World Bank.
- [22] World Bank. (2024). *Digital economy for Africa initiative: Progress and future priorities*. World Bank.
- [23] World Economic Forum. (2024). *Global cyber security outlook 2024*. World Economic Forum.