IIAR JOURNALS

Innovating Knowledge. Advancing Research.

IIAR Journal of Security, Peace, and Conflict Studies

Vol 1, No 1, 2026

Cybersecurity, Critical Infrastructure and National Security in Developing States: A Theoretical Framework of Dependence, Capacity and Deterrence in the Digital Domain

Atolagbe Umar Kawu[1], NWOGBOJI Emmanuel Usulor[2], Igwe Emmanuel Sunday[3]

[1,2,3] Veristzon Global Research Lab

ABSTRACT

Developing states are digitising their financial systems, power grids, identity systems and government services faster than they are building the capacity to defend them, and they do so on hardware, software, cables and cloud infrastructure supplied by foreign firms and states. This theoretical paper develops a framework for cybersecurity as a national-security problem under conditions of dependence. Drawing on security studies and deterrence theory, on the literatures on cyber statecraft and strategic competition, on the cyber-capacity-building and cyber-diplomacy scholarship, on research on critical-infrastructure resilience, and on recent work on cybersecurity, cybercrime and digital sovereignty in Africa, it distinguishes three dimensions of the problem, dependence (the state does not control the systems it relies on), capacity (it cannot reliably detect, attribute or respond to intrusions) and deterrence (it cannot credibly threaten retaliation), and shows that the classical deterrence framework is largely unavailable to such states, whose security must instead rest on resilience, international cooperation and the deliberate management of dependence. The paper derives seven propositions about the conditions under which digitisation increases or reduces national vulnerability, about the relationship between cybercrime, which is largely a domestic governance problem, and cyber conflict, which is an international one, and about the institutional architecture appropriate to capacity-constrained states. Nigeria's financial system, power sector and digital-identity infrastructure anchor the analysis. The paper closes with implications for national cybersecurity strategy, capacity-building partners and research. It concludes that developing states should stop asking how to deter cyber attack and start asking how to remain functional when it occurs, how to govern the systems on which they depend, and how to protect their citizens from the crime that does them most harm, building security on redundancy, competence and cooperation rather than on a threat of retaliation they cannot credibly make.

Keywords: cybersecurity; critical infrastructure; national security; cyber capacity; deterrence

Cybersecurity, Critical Infrastructure and National Security in Developing States: A Theoretical Framework of Dependence, Capacity and Deterrence in the Digital Domain

1. INTRODUCTION

The security of a modern state now depends on systems it rarely builds and often does not control. Payments clear through digital networks; electricity is dispatched through control systems; citizens are identified through biometric databases; tax, health and social-protection services run on software. In developing states these systems have been adopted rapidly, frequently leapfrogging the analogue infrastructure that preceded them in richer countries, and they have been adopted on hardware, software, undersea cables and cloud services supplied by foreign firms and, in some cases, foreign states (Mwema & Birhane, 2024; Hossain & Mahmud, 2026). The result is a pattern of national exposure that the security-studies literature, developed for powerful states that design and control their own digital infrastructure, does not adequately describe.

The dominant frameworks for thinking about cyber threats at the national level were built around the question of how powerful states deter one another in cyberspace. That literature has moved from the application of classical deterrence theory, through scepticism about whether deterrence works at all in the cyber domain, to accounts of cyber operations as persistent strategic competition below the threshold of armed conflict (Akoto, 2026a, 2026b). Its concerns, escalation between great powers, the attribution of sophisticated state operations, the calibration of offensive capability, are real, but they are not the concerns of most developing states, which neither possess significant offensive cyber capability nor face cyber threats primarily from rival states.

This paper develops a framework for cybersecurity as a national-security problem in developing states. It distinguishes three dimensions, dependence, capacity and deterrence, and argues that the third, which dominates the literature, is the least available to such states and the least relevant to their security. Their security must instead be built on resilience, cooperation and the deliberate management of dependence. The paper derives propositions about when digitisation increases or reduces national vulnerability, distinguishes cybercrime from cyber conflict as security problems with different institutional requirements, and considers the architecture appropriate to capacity-constrained states, with Nigeria as the anchoring case.

The analysis begins with the deterrence debate and its limits, then develops the three-dimension framework of dependence, capacity and deterrence and applies it to three critical sectors. It distinguishes cybercrime from cyber conflict as security problems with different institutional requirements, proposes resilience as the organising principle, and derives a set of propositions, before anchoring the argument in Nigeria's financial, identity and power systems and drawing out its implications.

2. LITERATURE REVIEW

2.1 Deterrence in Cyberspace and Its Limits

From deterrence to competition

The first generation of thinking about national cybersecurity applied the logic of nuclear and conventional deterrence: a state deters attack by threatening unacceptable retaliation (deterrence by punishment) or by making attack futile (deterrence by denial). The application ran into well-known difficulties. Attribution of cyber operations is slow and uncertain, so that retaliation cannot reliably be aimed; the threshold at which a cyber operation warrants response is unclear; and much state cyber activity consists of espionage and the preparation of access rather than destructive attack. Akoto (2026a) argues that state-sponsored cyber conflict is better understood as intelligence-driven strategic competition than as a form of warfare to be deterred, with the consequence that treating every intrusion as a failure of deterrence misreads what is happening. Akoto (2026b), examining why some states become persistent practitioners of offensive cyber operations while others remain occasional attackers, finds that sustained offence emerges only after states surpass substantial fixed costs and capability thresholds and institutionalise offensive units within their security apparatus, a finding that places most developing states firmly on the side of targets rather than practitioners.

Small states and asymmetry

A strand of the literature asks whether states without great-power capability can deter at all. Li (2024) argues that small states can achieve a form of cyber deterrence through a defence-centric strategy that exploits asymmetric advantages: a smaller attack surface, faster incident response and cohesive populations, illustrated by Estonia and Singapore.

© IIARJournal. All rights reserved.

The argument is instructive for developing states precisely because its conditions do not transfer. Large developing states such as Nigeria have large and rapidly expanding attack surfaces, slow and fragmented incident response, and the institutional and social cohesion that Estonia and Singapore draw on is not a given. The advantages Li identifies are advantages of small, wealthy, high-capacity states, not of states that are populous, digitising rapidly and capacity-constrained.

What the debate omits

The deterrence debate omits three features of the developing-state condition. It assumes that the state controls the systems it seeks to defend. It assumes the capacity to detect and attribute intrusions. And it treats the threat as coming principally from other states, when for developing states the larger volume of harm comes from criminal actors, many of them domestic. The framework that follows is built around these omissions.

2.2 Three Dimensions: Dependence, Capacity, Deterrence

Dependence

Dependence is the condition of relying on digital systems the state does not control. It takes several forms. Physical dependence arises from infrastructure owned and operated by others: Mwema and Birhane (2024) show that the undersea cables on which African connectivity depends are increasingly built and owned by large technology corporations, and describe this as a new frontier of digital colonialism in which the physical backbone of the continent's internet is controlled from outside it. Technological dependence arises from reliance on foreign hardware and software, whose vulnerabilities the state cannot audit and whose update cycles it does not set. Hossain and Mahmud (2026) analyse cybersecurity vulnerability in the Global South as structurally linked to external technology dependence, including dependence on foreign providers for building national cyber capacity and incident-response capability itself. Political dependence arises where infrastructure is supplied through state-to-state arrangements: Lin (2024) and Da Vinha (2024) examine the supply of Chinese digital and surveillance infrastructure to African states and the questions of control it raises, and Johansen and Kruck (2025), writing about military artificial intelligence, describe a competence–control trade-off in which states that rely on private experts for technical capability cede control over the systems those experts build. Each form of dependence limits what the state can know about, and do to protect, its own critical systems.

Capacity

Capacity is the ability to prevent, detect, attribute, respond to and recover from cyber incidents. It comprises skilled personnel, institutions with clear mandates, legal frameworks, technical tools, information-sharing arrangements and the funding to sustain them. Developing states face shortfalls in all of these, and the shortfalls interact with dependence: a state that lacks the personnel to audit foreign systems cannot reduce its dependence on the vendors that supply them. Capacity-building has become a major field of international cooperation; Rodríguez Acosta (2026) proposes a framework for sustainable cyber-diplomacy capacity building that attends to institutional governance and human-resource development, implicitly acknowledging that much capacity-building to date has been episodic and donor-driven. Avordeh and Ofori-Boateng (2026), examining cybersecurity risks in residential demand response for smart grids in sub-Saharan Africa, show how the extension of digital control into energy systems creates exposures that utilities and regulators are not yet equipped to manage.

Deterrence

Deterrence is the ability to dissuade attack by threat. For developing states it is largely unavailable. Deterrence by punishment requires offensive capability and reliable attribution, both of which most developing states lack (Akoto, 2026b). Deterrence by denial requires defensive capability sufficient to make attack futile, which is a function of capacity and of control over one's systems, both of which are constrained. And the most numerous threats, criminal groups seeking financial gain, are not deterred by threats of state retaliation in any case; they are deterred, if at all, by the probability of detection and prosecution, which is a matter of law enforcement rather than strategy.

The interaction

The three dimensions form a hierarchy for developing states. Dependence constrains capacity, because a state cannot defend what it cannot inspect. Capacity constrains deterrence, because a state cannot deny or punish what it cannot detect and attribute. Strategies that begin from deterrence, acquiring offensive cyber units, declaring retaliatory doctrines, therefore begin at the wrong end. The effective sequence runs the other way: manage

© IIARJournal. All rights reserved.

dependence, build capacity, and let whatever deterrent effect is achievable emerge from demonstrated resilience.

2.3 Three Critical Sectors

The three dimensions take different forms in different sectors. Three sectors are central to the security of rapidly digitising developing states: finance, identity and energy. Each has been digitised quickly, each depends on imported systems, and each fails in a different way.

Finance

Digital finance, bank transfers, card payments, mobile money and the switches that connect them, has been the most dynamic sector of digitisation in much of Africa and the foundation of financial-inclusion policy. Its security problem is predominantly criminal: fraud, account takeover, insider abuse and attacks on payment switches for financial gain. Its incentives for security are comparatively strong, because losses fall on firms with the resources and the regulatory obligation to invest in defence, and because central banks can impose standards on a small number of large institutions. Its distinctive risk is concentration: a small number of switches, processors and cloud providers carry a large share of transactions, so that a failure at one point can halt commerce across a country. The security of digital finance is therefore less a matter of deterring adversaries than of supervising concentration and ensuring that payments can continue, by manual or alternative channels, when a node fails. Its social stakes are high because, as Auwal and Lazarus (2025) show for Nigeria, the experience of fraud erodes the trust on which inclusion depends.

Identity

Digital identity systems, biometric registries linked to banking, telecommunications, voting and social protection, are the newest and in some respects the most sensitive critical infrastructure. A breach of a payment system loses money; a breach of an identity system loses the permanent, unchangeable biometric markers of a population. Identity systems also concentrate political dependence: they are frequently designed, financed or supplied by external partners whose objectives may differ from those of the citizens enrolled. Iwuoha (2025) examines a European-funded biometric identity programme in West Africa situated between the European Union's external border securitisation and the ECOWAS commitment to free movement, illustrating how the purposes built into an identity infrastructure may be set outside the region it serves. Identity systems are thus exposed on all three dimensions at once: they depend on external suppliers and funders, they require security capacity that registration agencies rarely possess, and their compromise cannot be deterred or reversed.

Energy

Energy systems are being digitised through supervisory control and data acquisition, smart metering, distributed generation and demand response. Their security problem combines criminal and strategic threats: ransomware against utilities, theft through meter manipulation, and the possibility of state-linked actors preparing access to control systems for use in crisis. Rotibi et al. (2025) show that operational cyber risk in industrial control systems must be identified at the level of the system rather than the component, because failures propagate through interactions that component-level assessment misses. Avordeh and Ofori-Boateng (2026) show that the extension of demand response to households in sub-Saharan African smart grids creates new exposures for utilities and regulators unprepared to manage them. In states where the grid is already fragile, a cyber incident need not be sophisticated to cause disproportionate harm, because there is little spare capacity to absorb it.

Sectoral implications

The sectoral differences matter for strategy. Finance is the sector with the strongest incentives and the most regulatory leverage, and its priority is resilience against concentration and fraud. Identity is the sector with the highest stakes and the least reversibility, and its priority is minimisation, collecting and linking only what is necessary, together with control over suppliers. Energy is the sector where cyber and physical fragility compound, and its priority is segmentation of control systems and manual fallback. A national strategy that treats critical infrastructure as a single category will misallocate effort among them.

2.4 Cybercrime and Cyber Conflict

Two problems

National cybersecurity discourse in developing states often fuses two problems that have different causes, different perpetrators and different remedies. Cyber conflict is the use of cyber operations by states and their proxies against other states: espionage, sabotage, influence operations and the preparation of access to critical systems.

© IIARJournal. All rights reserved.

Cybercrime is the use of digital systems by criminal actors for financial or other gain: fraud, theft, extortion, ransomware. For powerful states, cyber conflict is the strategic priority. For most developing states, cybercrime is the larger and more immediate source of harm, though cyber conflict carries tail risks to critical infrastructure.

The domestic dimension

Cybercrime in developing states is frequently domestic in both perpetration and victimisation, a point obscured by international attention to fraud schemes that target foreign victims. Auwal and Lazarus (2025), studying the experiences of local victims of the online fraud associated with the so-called Yahoo Boys in Nigeria, show that the harms of such crime fall on Nigerians as well as on foreigners, and that the social and economic damage to local victims is substantial. This matters for national security because the trust on which digital financial inclusion, e-government and the digital economy depend is eroded most directly by the fraud citizens experience, not by the state operations that dominate strategic discussion.

Different institutions

The two problems require different institutional responses. Cybercrime is addressed by law enforcement, prosecution, financial regulation, consumer protection and international legal cooperation; its success is measured in detection, conviction and victim recovery. Cyber conflict is addressed by intelligence, defence, diplomacy and critical-infrastructure protection; its success is measured in resilience and the absence of strategic surprise. Fusing them under a single national-security frame has costs. It securitises what is largely a criminal-justice problem, drawing intelligence and military institutions into domestic policing, and it can justify measures, surveillance, data retention, speech restrictions, whose primary effect falls on citizens rather than on adversaries. Osimen et al. (2026) examine the tension between national cybersecurity policy and citizens' rights in Nigeria, and Achinivu (2025) analyses the domestic drivers of digital authoritarianism there; both point to the risk that the securitisation of cyberspace serves state control as much as national security.

2.5 Resilience as the Organising Principle

From prevention to resilience

If deterrence is unavailable and prevention is never complete, the organising principle of developing-state cybersecurity must be resilience: the capacity of critical systems and the institutions that run them to continue functioning under attack, to contain damage, and to recover quickly. Hilger (2026) argues that the limitations of traditional cybersecurity frameworks, focused on prevention and control, have become evident as threats grow in complexity, and proposes a multidimensional framework for planning, assessing and governing cyber resilience as an organisational function. Osei-Kyei et al. (2023), in a systematic review of critical-infrastructure resilience indicators, identify the standards against which resilience can be measured and note their potential use by developing countries to benchmark the resilience of their infrastructure.

Components of resilience

Resilience in the developing-state context has four components. Redundancy means that the failure of one system or supplier does not disable a critical function: multiple cable landings and routes, manual fallbacks for payment and power dispatch, offline copies of identity and registry data. Segmentation means that intrusion into one network does not propagate to others: the separation of operational control systems from business networks, and of critical government systems from general administrative ones. Recovery capacity means tested plans, backups and personnel able to restore systems quickly. And institutional coordination means that operators of critical infrastructure, regulators, law enforcement and the national incident-response function share information and act together.

Managing dependence

Resilience also requires the deliberate management of dependence rather than its denial. Developing states cannot build their own cables, chips and cloud platforms, but they can diversify suppliers, require audit and disclosure rights in procurement, insist on in-country data storage for critical systems, and invest in the domestic expertise needed to inspect what they buy. The competence–control trade-off that Johansen and Kruck (2025) describe applies: the state that wishes to retain control over critical systems must retain sufficient competence to understand them. Mwema and Birhane (2024) and Hossain and Mahmud (2026) suggest that the terms of dependence are not fixed but negotiable, and that regional coordination increases the bargaining power of individual states.

Cooperation

© IIARJournal. All rights reserved.

Finally, resilience in states with limited capacity depends on cooperation: regional incident-response networks, information sharing with other states and with private operators, and participation in international capacity-building. Rodríguez Acosta (2026) emphasises that sustainable capacity-building must build institutions rather than deliver episodic training. Cooperation is also the only realistic substitute for the deterrence that developing states cannot achieve alone: collective attribution and response by groups of states raise the cost of attack in a way no single capacity-constrained state can.

3. CONCEPTUAL FRAMEWORK

Proposition 1. Digitisation of critical functions increases national vulnerability in proportion to the gap between the rate of adoption and the rate of capacity-building, and the gap is widest in states that adopt rapidly on foreign-supplied systems (Hossain & Mahmud, 2026). Proposition 2. Dependence on foreign-controlled physical, technological and political infrastructure constrains defensive capacity independently of resources, because a state cannot defend systems it cannot inspect; the constraint is relaxed only by retaining domestic competence sufficient to audit what is acquired (Mwema & Birhane, 2024; Johansen & Kruck, 2025). Proposition 3. Deterrence by punishment is unavailable to states below the capability threshold for persistent offensive operations, and investment in offensive cyber capability by such states will yield little deterrent effect relative to equivalent investment in resilience (Akoto, 2026b; Li, 2024). Proposition 4. The asymmetric defensive advantages available to small, high-capacity states, small attack surface, rapid response, social cohesion, are not available to large, rapidly digitising developing states, whose security therefore depends more heavily on redundancy, segmentation and cooperation (Li, 2024). Proposition 5. In developing states, cybercrime imposes larger aggregate harm on citizens and on trust in digital systems than state-sponsored cyber operations, so that national cybersecurity strategies weighted toward cyber conflict will under-serve the population's security (Auwal & Lazarus, 2025). Proposition 6. Fusion of cybercrime and cyber conflict under a single national-security frame will extend surveillance and speech restrictions over citizens without commensurate gains against either criminal or state adversaries (Osimen et al., 2026; Achinivu, 2025). Proposition 7. Regional cooperation in incident response, attribution and procurement increases the resilience and bargaining power of capacity-constrained states more than equivalent national investment, because it pools scarce expertise and aggregates leverage over suppliers (Rodríguez Acosta, 2026).

The propositions are stated as conditional claims for comparative research and as design principles for strategy.

4. ANALYSIS AND DISCUSSION

4.1 Nigeria as an Anchoring Case

Rapid digitisation

Nigeria illustrates the developing-state condition at scale. It has one of Africa's largest digital economies, a banking system in which electronic and mobile payments have grown rapidly, a national digital-identity programme linking biometric identity to banking, telecommunications and government services, and a power sector in which digital control and metering are being extended. Each of these is critical infrastructure; each has been digitised quickly; and each depends substantially on imported hardware, software and services.

Dependence

Nigeria's connectivity depends on undersea cables landing on its coast, an infrastructure increasingly owned or financed by foreign technology firms of the kind Mwema and Birhane (2024) describe. Its banking and identity systems run substantially on foreign-supplied platforms, and identity infrastructure in the region has been shaped by external funders' purposes (Iwuoha, 2025); its smart-city and security systems include foreign-supplied components (Lin, 2024; Da Vinha, 2024). Proposition 2 applies: the state's capacity to defend these systems is bounded by its capacity to inspect them, which depends on domestic expertise that is scarce and frequently drawn abroad by higher salaries.

Capacity

Nigeria has developed national cybersecurity policy, cybercrime legislation and institutional arrangements for incident response and sectoral oversight, whose evolution over the decade to 2024 Osimen et al. (2026) examine. Capacity remains uneven across sectors: the financial sector, with strong commercial incentives and regulatory oversight, is better protected than the power sector or government administration. Proposition 1 predicts that vulnerability will be greatest where

© IIARJournal. All rights reserved.

digitisation has outrun capacity, and the power sector's extension of digital control, of the kind Avordeh and Ofori-Boateng (2026) analyse for sub-Saharan smart grids, is a leading candidate.

Cybercrime and the security frame

Cybercrime is Nigeria's most visible cyber problem, at home and abroad. Auwal and Lazarus (2025) show its domestic victims; international attention concentrates on its foreign victims. Proposition 5 implies that Nigerian cybersecurity strategy should weight cybercrime, through law enforcement capacity, financial-sector controls and victim support, more heavily than cyber conflict. Proposition 6 cautions against the alternative: Osimen et al. (2026) examine the tension between Nigeria's cybersecurity policy and citizens' rights, and Achinivu (2025) locates the drivers of digital authoritarianism in Nigeria's domestic politics; together they indicate that the framing of cyber threats as national-security matters can be used to justify measures whose effects fall on citizens rather than adversaries.

What would help

The framework suggests four priorities for Nigeria. First, adopt resilience as the organising principle of national cybersecurity strategy, with redundancy, segmentation and tested recovery for the financial, identity and power systems (Hilger, 2026; Osei-Kyei et al., 2023). Second, manage dependence deliberately: diversify suppliers, require audit rights and in-country data storage in procurement for critical systems, and invest in the domestic expertise needed to exercise those rights. Third, separate the institutional treatment of cybercrime from that of cyber conflict, strengthening law enforcement and financial regulation for the former and critical-infrastructure protection and diplomacy for the latter, while protecting civil liberties against the securitisation of ordinary online activity. Fourth, lead regional cooperation through ECOWAS and the African Union on incident response, information sharing and collective negotiation with technology suppliers, where Nigeria's weight gives it a natural role.

4.2 Implications

For national strategy

National cybersecurity strategies in developing states should be reorganised around resilience rather than deterrence, should treat dependence as a variable to be managed rather than a fact to be accepted, and should distinguish cybercrime from cyber conflict in institutional design. Investment in offensive capability should be weighed against its opportunity cost in resilience.

For capacity-building partners

Partners supporting cyber capacity in developing states should prioritise institutional sustainability over episodic training, support the retention of domestic expertise, and avoid tying capacity-building to the procurement of their own technology, which deepens the dependence the capacity is meant to manage (Rodríguez Acosta, 2026; Hossain & Mahmud, 2026).

For research

The cybersecurity of developing states is understudied relative to that of great powers. Research is needed on the incidence and cost of cyber incidents in African critical infrastructure, on the effectiveness of capacity-building, on the terms of dependence in infrastructure contracts, and on the civil-liberties effects of cybersecurity legislation. The propositions offer an agenda.

Limits

The paper is conceptual and relies on a thin empirical literature for African critical infrastructure. It treats developing states as a category when they differ greatly in size, capacity and dependence. And it does not address the cybersecurity implications of artificial intelligence, which is reshaping both attack and defence.

5. CONCLUSION AND RECOMMENDATION

The national cybersecurity problem of developing states is not a smaller version of the great-power problem. It is a different problem, defined by dependence on systems the state does not control, by capacity that lags behind digitisation, and by the near-unavailability of deterrence. This paper has developed a framework around those three dimensions, shown that they form a hierarchy in which dependence constrains capacity and capacity constrains deterrence, distinguished cybercrime from cyber conflict as security problems with different institutional requirements, proposed resilience as the organising principle, derived seven propositions, and anchored the analysis in Nigeria's financial, identity and power systems.

The conclusion is that developing states should stop asking how to deter cyber attack and start asking how to remain functional when it occurs, how to know and govern the systems they depend on, and how to protect their citizens from the crime that

© IIARJournal. All rights reserved.

does them most harm without sacrificing the freedoms that digital systems should serve. Security in the digital domain, for most of the world's states, will be built not on the threat of retaliation but on redundancy, competence and cooperation.

6. CONTRIBUTION TO EXISTING KNOWLEDGE

The paper contributes a decomposition of the national cybersecurity problem of developing states into dependence, capacity and deterrence, and shows that they form a hierarchy in which dependence constrains capacity and capacity constrains deterrence, so that the deterrence framework which dominates the literature is the least available to such states.

It further contributes a distinction between cybercrime and cyber conflict as security problems with different institutional requirements, and an argument for resilience as the organising principle, giving national strategists and capacity-building partners a basis for building security on redundancy, competence and cooperation rather than on a threat of retaliation these states cannot make.

7. REFERENCES

Achinivu, C. (2025). Understanding digital authoritarianism in Africa: The case of Nigeria. Journal of Contemporary African Studies, 43(3), 390–405. https://doi.org/10.1080/02589001.2025.2548785

Akoto, W. (2026a). Unpacking state-sponsored cyber conflict: Intelligence-driven strategic competition in cyberspace. Journal of Strategic Studies, 49(2), 320–347. https://doi.org/10.1080/01402390.2025.2602554

Akoto, W. (2026b). Cyber conflict as statecraft: Explaining the persistence of state-sponsored cyber operations. Journal of Global Security Studies, 11(1), ogag004. https://doi.org/10.1093/jogss/ogag004

Auwal, A. M., & Lazarus, S. (2025). Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria. Discover Psychology, 5(1), 161. https://doi.org/10.1007/s44202-025-00479-5

Avordeh, T. K., & Ofori-Boateng, D. (2026). Identifying and mitigating cybersecurity risks in residential demand response for smart grids in Sub-Saharan Africa. Utilities Policy, 101, 102223. https://doi.org/10.1016/j.jup.2026.102223

Da Vinha, L. (2024). Smart for whom? Africa's smart cities and digital authoritarianism. International Journal of Intelligence and CounterIntelligence, 37(3), 941–959. https://doi.org/10.1080/08850607.2023.2284629

Hilger, R. P. (2026). From cybersecurity to cyber resilience: A systemic and scalable approach for improving resilience and adaptive capacity. Journal of Cybersecurity, 12(1), tyag011. https://doi.org/10.1093/cybsec/tyag011

Hossain, D., & Mahmud, K. U. (2026). Growing digital orientation and cybersecurity vulnerabilities in the Global South: Analyzing dependency and geopolitical dimensions. Digital Policy, Regulation and Governance. Advance online publication. https://doi.org/10.1108/dprg-06-2026-0360

Iwuoha, V. C. (2025). European biometric ID program in West Africa: Between European external border securitization and ECOWAS free movement. African Security, 18(3), 229–260. https://doi.org/10.1080/19392206.2025.2491206

Johansen, A., & Kruck, A. (2025). The competence–control trade-off in military AI innovation: Autonomous weapons systems and shifting modes of state control over private experts. European Journal of International Security. Advance online publication. https://doi.org/10.1017/eis.2025.10020

Li, T. Y. (2024). Asymmetry in the digital age: Cyber deterrence strategies for small states. Journal of Strategic Security, 17(4), 71–88. https://doi.org/10.5038/1944-0472.17.4.2268

Lin, B. (2024). Beyond authoritarianism and liberal democracy: Understanding China's artificial intelligence impact in Africa. Information, Communication & Society, 27(6), 1126–1141. https://doi.org/10.1080/1369118x.2023.2239322

Mwema, E., & Birhane, A. (2024). Undersea cables in Africa: The new frontiers of digital colonialism. First Monday, 29(4). https://doi.org/10.5210/fm.v29i4.13637

Osei-Kyei, R., Almeida, L. M., Ampratwum, G., & Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. Construction Innovation, 23(5), 1210–1231. https://doi.org/10.1108/ci-03-2021-0047

Osimen, G. U., Wonosikou, M. H., & Odeigah, T. N. (2026). National cybersecurity policy and citizens' rights in Nigeria. The International Journal of Human Rights, 30(7), 1491–1516. https://doi.org/10.1080/13642987.2026.2619962

Rodríguez Acosta, J. E. (2026). A framework for sustainable cyber diplomacy capacity building. Journal of Cyber Policy, 11(1), 152–175. https://doi.org/10.1080/23738871.2026.2722913

Rotibi, A. O., Saxena, N., Burnap, P., & Read, C. (2025). System-level operational cyber risks identification in industrial control systems. Cyber-

© IIARJournal. All rights reserved.

Physical Systems, 11(3), 265–296. https://doi.org/10.1080/23335777.2024.2373388

© IIARJournal. All rights reserved.