Separating Damage, Complexity and Criticality in African Cyber Incidents: An Evidence-Constrained Framework with Twelve Illustrative Cases[1]

János Besenyő[2], Máté Attila Kovács[3]

Abstract:

Public discussion of cyber incidents tends to merge four separate questions: whether a target is socially important, whether an attack was technically complex, whether systems were exposed or compromised, and whether the event caused real operational harm. In African analysis this blurring is costly, because public reporting is highly uneven. The article develops a closed framework around three instruments built and tested on 15,789 event records in the Maryland Cyber Events Database: the Damage Severity Index (KSM), an ordinal measure of technical-operational consequence; the Complexity Index (KoI), a transparent sum of observable persistence, lateral movement, evasion and multi-stage execution; and the Criticality Indicator (KrI), which flags critical-sector status without inflating severity. Rather than a new composite score, it adds two evidential rules: functional criticality is described apart from legal sector labels, and missing technical detail is recorded as not assessable rather than as absence. Twelve public incidents illustrate the approach: severe operational disruption can coincide with sparse reporting, data compromise can be serious without equivalent service interruption, and socially essential digital services can be critical outside conventional utility categories. The framework thus supports consistent comparison without letting importance, identity or reputation replace evidence.

Keywords:
African Critical Infrastructure; Cyber Incident Measurement; Damage Severity Index; Complexity Index; Functional Criticality; Mobile Money; Public Digital Services; Evidence Quality; Missingness; Ransomware.

[1] DOI: 10.12700/jceeas.2026.6.3.559

[2] Professor and Head of the Africa Research Institute, Óbuda University, Budapest, Hungary; Visiting Professor, Centre for Military Studies (CEMIS), Stellenbosch University, Republic of South Africa; ORCID: 0000-0001-7198-9328; besenyo.janos@uni-obuda.hu.
[3] PhD-Student, Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary; ORCID: 0000-0001-5088-5749; kovacs.attilamate@uni-obuda.hu.

1. Introduction

Cybersecurity in critical infrastructure is usually discussed in terms of threats, vulnerabilities and attackers, yet the question that matters most to operators and public authorities is what an event actually did. A vulnerability may sit unexploited for years; a compromise may occur with no lasting interruption to operations; a denial-of-service attack can take a socially important portal offline while the underlying records remain untouched. A ransomware label, similarly, describes how a piece of malware behaves without telling anyone whether the incident reached operational technology, a clinical workflow or payment settlement, or stayed inside a limited administrative segment. These are not semantic differences. They decide whether an incident calls for an information-security response, a business-continuity response, a safety response, or some combination of the three. Work on critical-infrastructure resilience treats continuity, layered protection and organisational preparedness as separate from the naming of threats (Kovács, 2024a, 2024b).

The analysis here rests on three instruments defined at the level of the individual incident: the Damage Severity Index (KSM), an ordinal 1–5 measure of documented technical-operational consequence; the Complexity Index (KoI), a 0–4 sum of four observable attack behaviours; and a separate Criticality Indicator (KrI) for critical-sector status. All three were constructed and tested on the Maryland Cyber Events Database (MCED), a manually reviewed corpus of publicly reported cyber events maintained by the Center for International and Security Studies at Maryland (CISSM, n.d.-a, n.d.-b; Kovács, 2026). Their governing rule is that consequence, sophistication, sector importance and actor category must not define one another: an incident is not severe because it hit a utility; an attack is not complex because it has been attributed to a state; and a service is not a confirmed vulnerability because an automated scanner raised a warning.

This separation is especially useful for African cases. Digital transformation across the continent is rapid but uneven, touching telecommunications, finance, government, energy, health and logistics at very different speeds. The African Union's Digital Transformation Strategy treats digital infrastructure, digital government, digital financial services, digital health, digital identity, cybersecurity and data protection as interdependent parts of development (African Union, 2014, 2020, 2024). Mobile technologies contributed 140 billion US dollars, or 7.3% of gross domestic product, in Sub-Saharan Africa in 2023, and mobile-money systems now carry household, commercial and public-service transactions on a scale that makes their resilience a societal matter rather than a narrow application-security concern (GSMA, 2024, 2026). The World Bank likewise frames affordable, productive use of digital technology as a route to employment and economic transformation (World Bank, 2023).

The evidence available for the region is uneven in ways that matter for measurement. The Global Cybersecurity Index scores national commitment across legal, technical, organisational, capacity-building and cooperation pillars, but it does not measure how frequent or how severe attacks actually are (International Telecommunication Union, 2024). INTERPOL's Africa Cyberthreat Assessment draws on member-country reporting and partner evidence to describe threats such as scams, ransomware, business email compromise and digital extortion, yet it is not an incident-level, regionally balanced

corpus (INTERPOL, 2025). What reaches the public record depends on regulation, media access, institutional incentives, language and whether a forensic investigation was even possible. When a report says nothing about lateral movement, that may mean lateral movement did not happen, or that the investigation was limited, the detail withheld, or the statement written only to reassure users.

The article therefore sets itself a bounded question: how can publicly documented African cyber incidents be read consistently, without letting visibility, sector status, country identity or an attacker's reputation stand in for measured harm and observable behaviour? The answer offered here is an evidence-constrained framework resting on four rules. Damage is assigned only from documented technical-operational consequence. Complexity is assigned only from observable behaviours, and is left unscored where the source record does not support it. Legal and functional criticality are recorded outside the damage scale. And the strength of the source, together with any remaining uncertainty, travels with every conclusion. The twelve incidents that follow illustrate what these rules buy in practice; they are worked examples, not a representative sample, and they support no claim about how common any of this is across the continent.

Measured against the original MCED analysis (Kovács, 2026), the contribution of this article is specific. The constructs and the coefficients summarised in Section 3 belong to that earlier work. What is added here is the explicit three-state treatment of evidence, which stops missing technical detail from being read as absence; the functional-criticality layer, which complements legal sector classification; and the structured application of the three instruments to publicly documented African incidents. These are methodological adaptations demonstrated on twelve cases, not independently validated new scales.

2. The Measurement Problem: Four Concepts That Should Not Be Merged

A typical incident account starts from the organisation and the attacker: a hospital hit by ransomware, a central bank attacked, a government portal taken offline, a telecommunications operator leaking data. That form works for news reporting but is analytically thin, because it leaves four things tangled together: exposure or compromise, technical complexity, operational damage, and criticality. To compare incidents properly, each of these has to answer a different question.

Exposure and compromise describe what was technically reachable or affected, and on their own they do not settle consequence. An internet-facing service, an out-of-date software version or a stolen dataset can all represent serious risk, but the actual effect still has to be established. The reverse also happens: an organisation can suffer major operational disruption even when the public record carries little forensic detail. Keeping this dimension distinct guards against two opposite mistakes, reading unverified exposure as confirmed harm, and playing down a severe service interruption because the technical story is thin.

Complexity describes observable characteristics of how an attack was carried out. KoI uses four binary components mapped conceptually to MITRE ATT&CK: persistence,

lateral movement, defence or detection evasion, and multi-stage execution (MITRE, n.d.). These were chosen because each can be traced back to evidence rather than inferred from an attacker's reputation or from the fear a label evokes. A ransomware event does not earn a high KoI by default; ransomware is a broad operational category, not proof of a complete intrusion sequence (Kovács, 2022b). Encryption may be the last stage of a long intrusion, yet the public source may say nothing about initial access, dwell time, privilege escalation, internal movement or evasion. If every unknown component were scored as zero, under-investigated or under-reported events would automatically look technically simple.

Damage describes the technical-operational outcome that was actually realised. KSM is a five-level ordinal proxy, adopted because comparable financial figures are rarely made public. The lower levels cover contained or short-lived technical effects; the higher levels cover sustained service interruption, system-wide unavailability and physical-operational consequences, with KSM=5 reserved for a documented physical-operational effect. What matters here is that the scale is independent of sector. A data breach at a social-security institution can carry deep privacy and trust consequences and still sit below the damage level of an event that halts laboratory processing or port operations. That does not make the breach less important; it simply means confidentiality loss and operational damage are different outcomes and should be recorded as such.

Criticality asks why the affected function matters to society. KrI is kept separate from KSM and KoI and rests on critical-sector classification. In African settings a purely legal sector label may not capture the real dependence on a service. Mobile money, digital identity, government service portals, prepaid electricity vending and central-bank payment infrastructure can be socially essential because large populations, or several dependent services, have no realistic substitute for them. Functional criticality should therefore complement the legal classification, but it must stay out of KSM. Folding it in would make the analysis circular: a service would be judged highly damaging because it is critical, and then judged critical because its assigned damage is high.

A cross-cutting dimension is the quality of the evidence itself. Analysis based on public sources records not only what happened but also what could be observed and disclosed. Each coded state should therefore distinguish confirmed present, confirmed absent and not assessable. The same care is needed in low-noise technical validation, where silence from a probed host at a given time is not proof that a service is absent, and an automated candidate finding is not a validated vulnerability. Applied to incident reports, 'no published evidence of persistence' is not the same as 'persistence absent'. The framework is intentionally cautious on this point: where the record is insufficient it prefers an explicit unknown to a precise-looking score.

Why these instruments rather than others is a fair question, and the answer lies in fit. Any measure intended for African incident comparison has to satisfy three conditions: it must work from public reporting, because that is usually all there is; it must keep damage, complexity and criticality apart, because they answer different operational questions; and it must handle missing detail explicitly, because disclosure varies more than incident reality does. The familiar candidates each fail at least one of these. CVSS scores vulnerabilities, not incident consequence. Financial-loss figures are rarely disclosed

and rarely comparable. National indices measure state commitment, not events (International Telecommunication Union, 2024). Composite risk scores merge the very dimensions that need separating. KSM, KoI and KrI were built for exactly this evidence class, public event-level reporting, and have been tested on it at scale; Section 3 summarises the empirical behaviour that makes them usable here.

3. The Measurement Instruments

3.1 How the Instruments Behave on Large-Scale Data

The instruments were developed on 15,789 MCED records spanning January 2014 to October 2025; after cleaning and the removal of records with an undetermined actor label, 15,166 incidents supported the severity and complexity tests, and 14,938 formed the predictive sample over the three sufficiently represented actor categories (Kovács, 2026). The analysis behind them was longitudinal and incident-level, with temporally separated training, validation, calibration and out-of-time testing rather than a random split, so the reported performance reflects prediction on genuinely later events.

Three tested properties matter for how the instruments are used here. First, the top of the damage scale discriminates. In the MCED Utilities category 10.07% of incidents reached KSM=5, against 0.28% outside it; a year-controlled logistic regression put the odds ratio at 40.52 (95% CI 23.83–68.92) with discrimination of AUC=0.892 (Kovács, 2026). The figure expresses the conditional odds of a documented physical-operational effect given an attack in that category, not a claim that utilities are attacked forty times more often, and it is not an estimate for Africa. What it establishes for present purposes is that KSM=5 marks a rare, well-separated outcome class rather than a rhetorical superlative.

Second, complexity can be scored without attribution. Across actor classes the four KoI components differ significantly, with Welch's $F=342.67$ ($p<0.00001$) and Cliff's delta=0.42 for the state versus non-state comparison (Kovács, 2026). This does not mean sophisticated operations must be state-sponsored. It means the components register real differences in observed behaviour, so complexity need not be inferred from an attacker's reputation.

Third, on this data simpler prediction won. On the out-of-time test period a rule-based baseline reached Macro-F1=0.6429, logistic regression 0.7678, and a stacking ensemble only 0.6439; the logistic model improved on the rule baseline by 19.4% in relative terms while remaining interpretable (Kovács, 2026). That result carries directly into this article's design choices: no composite index, no free parameters, and explicit abstention where evidence is missing, because added machinery has to demonstrate benefit before it earns its complexity.

3.2 The Four-Part Incident Representation

Each incident is represented through four linked fields that cannot substitute for one another:

- **KSM – realised damage:** an ordinal 1–5 placement based on documented technical-operational consequence. The placement is provisional when the public record does not support a precise level.

- **KoI – observable complexity:** a 0–4 sum, formed only when persistence, lateral movement, evasion and multi-stage execution can each be assessed. Where they cannot, the relevant components stay not assessable and no total is forced.
- **KrI and functional criticality:** a separate description of legal sector status and of the societal function of the affected service, covering dependence, replaceability, concentration and the availability of manual alternatives.
- **Evidence state:** the source basis, the confidence, and the reason for any missingness attached to each conclusion. Official post-incident reports and operational records carry more weight than attacker claims or unattributed summaries.

For the illustrative coding in this article, KSM is assigned to the highest consequence level directly supported by the documented event, never to a hypothetical worst case, using the following anchors. KSM=1 covers a confirmed technical security event with no documented effect on services. KSM=2 covers partial or contained disruption of selected applications, where the sources document a partial effect rather than the loss of a function to its users, and confirmed data compromise without documented material service interruption. KSM=3 covers the documented loss of a public-facing service, or of a specific service function, to its users, or a complete internal outage with bounded operational effect, while core institutional functions continue. KSM=4 covers sustained or system-wide interruption of core institutional services, including national payment or vending functions, without documented physical-process effect. KSM=5 is reserved for a documented physical-operational consequence, such as halted port logistics or interrupted laboratory processing. The boundary between KSM=2 and KSM=3 is therefore set by the documented extent of the interruption (partial disruption of selected applications as opposed to the loss of a function to its users), not by the importance of the affected service, which belongs to the criticality layer. Confidentiality loss is recorded separately and does not, by itself, justify a placement above KSM=2. A single level is assigned only where the documented consequence meets one anchor; a range is reported only where the record supports two adjacent anchors. These anchors guide the illustrations and are not a substitute for the full coding specification of the original analysis (Kovács, 2026).

Each KoI component is coded as present only on an explicit statement in a cited source: persistence requires a maintained foothold or documented re-entry; lateral movement requires spread beyond the initially affected segment; evasion requires disabled or bypassed defences; multi-stage execution requires a described sequence of distinct phases. A component is coded as absent only on affirmative evidence ruling it out within the scope of the investigation; silence in a press statement counts as neither. Where any component is not assessable, no 0–4 total is formed. For these illustrative cases, Tables 1 and 2 summarise the available complexity evidence and its limitations rather than presenting a complete component-level coding matrix. Malware family, a DDoS label and claimed actor identity are not proxies for any component.

These fields are kept apart on purpose rather than collapsed into one overall score. A single composite number would hide whether the concern comes from high realised damage, high technical complexity, critical societal dependence, weak evidence, or some mix of these, and operational decisions turn on exactly that difference. A port

operator facing KSM=5 disruption with an unknown KoI needs recovery and continuity measures at once, whatever remains unresolved about attribution or intrusion depth. A social-security institution facing a large confidentiality breach but limited service interruption needs a privacy response, credential-risk management and public communication, even though its KSM placement is lower.

The framework also holds event consequence apart from recovery context. Manual fallback, backup power, analogue procedures, alternative providers, spare parts, institutional coordination and the speed of restoration all shape how a society experiences an incident. None of them changes what the attack technically did, but they explain why two events at the same KSM can differ in duration and social reach. This matters most where digital and physical infrastructure sit side by side with uneven redundancy.

4. Materials and Analytical Procedure

The article uses twelve purposively selected incidents from 2020–2025 to show the framework at work across different functions and consequence types. The cases span South, East, West and North Africa and cover logistics, health, justice, legislative administration, electricity distribution, digital government, mobile money, central banking, telecommunications, social security and public websites. A case was included when an official statement, institutional report, regulator document, peer-reviewed account or established news source described at least the target, the timing and a confirmed consequence. The set was chosen for conceptual variety, not statistical representation.

Selection drew on public reporting of African cyber incidents from 2020–2025 across government and institutional statements, regulator publications, annual reports, peer-reviewed accounts and established international news services. Inclusion required an identifiable African target or affected service, an identifiable period, and a publicly documented operational, availability or confidentiality consequence from at least one attributable source. Incidents supported only by attacker claims, leak-site listings or uncorroborated aggregation were excluded. From the documented candidates, the twelve were chosen purposively so that the four regions and the consequence types distinguished in Section 2 are each represented: physical-operational effect, sustained service interruption, availability disruption, confidentiality loss and third-party transmission. No claim is made that they exhaust the incidents meeting these conditions, and no screening denominator or rejected-case register was produced. Public reporting itself reflects disclosure practice rather than incident reality, which is a further reason the set supports illustration and not prevalence estimation.

The order of preference among sources was cautious. Official operational and annual reports came first, since they establish the state of a service and the organisation's response. Peer-reviewed medical analysis was used to read the clinical implications of the South African laboratory incident. Regulator statements were used where they confirmed a telecommunications incident. Reputable news reporting was used where it quoted an official statement, or where the event concerned the temporary availability of a public website. Attacker claims were never the sole basis for a judgement about impact or attribution.

Each case was worked through the same four questions in order. What consequence is directly documented? What provisional KSM level, or narrow band, is consistent with it? Which KoI components can actually be established from the source record? And what legal or functional dependency makes the service critical, while which contextual factor limits or amplifies the outcome? Taking them in this order stops the importance of the organisation from fixing the severity in advance, and stops the name of a threat group or malware family from fixing the complexity in advance.

The KSM placements in Figures 1 and 2 are therefore analytical illustrations, not adjudicated dataset labels. A range is reported only where the public record supports two adjacent anchors. KoI appears mainly as an evidence state, because most public institutional communications do not publish the internal technical detail a defensible 0–4 total would require. The method refuses to turn missing information into a zero. Nothing about prevalence, regional ranking, causation or model performance is drawn from the twelve cases.

Reliability was handled in two layers. For fixed structured MCED inputs and a fixed rule-based mapping, the derivation of KSM and KoI in the original analysis is deterministic and involves no additional inter-coder judgement at that calculation stage (Kovács, 2026). The twelve case placements here are provisional, author-derived interpretations of the cited public sources; the level anchors in Section 3.2 were made explicit during revision and the placements were re-checked against them. No independent multi-coder assessment was conducted, and no inter-rater agreement coefficient is therefore reported (Cohen, 1960). A subsequent reproducibility study on a larger African corpus should give independent coders the same source material and coding definitions, record scores before reconciliation, and report agreement separately for the ordinal KSM levels and the categorical KoI component states.

5. Twelve illustrative African Incidents

The cases below show how one framework reaches different conclusions for availability disruption, physical-operational effect, confidentiality loss and third-party dependency. “Not assessable” means the cited public sources do not give enough evidence to code the relevant KoI components; it does not mean those behaviours were absent.

Incident	Documented consequence	Provisional KSM	KoI / evidence note
Transnet, South Africa (2021)	A cyber incident disrupted port/container operations; manual processes and force majeure were reported before full port operations were restored.	5	Operational effect is confirmed; public sources do not support a complete KoI.
NHLS, South Africa (2024)	Ransomware severely affected IT systems, laboratory processing and result delivery, jeopardising continuity of diagnostic services.	5	Ransomware is confirmed, but persistence / lateral movement / evasion are not fully public.

Incident	Documented consequence	Provisional KSM	KoI / evidence note
Department of Justice, South Africa (2021)	The incident shut down departmental IT systems and disrupted digital justice administration; one official report records four months of ICMS unavailability.	4	Sustained system-wide service effect; KoI not assessable from public reporting.
Western Cape Provincial Parliament (2023)	A ransomware attack rendered servers inoperable and internal ICT services inaccessible, while parliamentary business continued through response and fallback arrangements.	3	Material technical disruption with bounded operational effect; KoI not assessable.
Electricity Company of Ghana (2022)	The company later confirmed ransomware and approximately one week of inability to vend prepaid electricity, with major revenue and operational consequences.	4	Payment / vending operations were impaired; no confirmed grid-process manipulation is established.
eCitizen, Kenya (2023)	A DDoS attack caused downtime in the national digital-government platform; services resumed and public statements reported no data breach.	3	Availability attack is documented; complexity beyond distributed traffic is not assessable.

Figure 1. Illustrative cases 1–6.

Incident	Documented consequence	Provisional KSM	KoI / evidence note
Pegasus / MTN Uganda integration (2020)	A third-party aggregator breach affected Bank-to-Wallet transfers; selected inter-network functions were suspended while core MTN Mobile Money services remained intact.	3	Third-party concentration transmitted impact without full core-platform compromise.
Bank of Zambia (2022)	A cyber incident disrupted selected IT applications; the public website was down for part of several days and a monitoring system was affected, while core systems remained up.	3	Public-facing website outage documented, core systems held; KoI not assessable from the cited public sources.
Central Bank of Lesotho (2023)	A cyber incident led to isolation or suspension of systems and disruption of national payment services before restoration.	4	High functional criticality and payment-system interruption; intrusion detail remains limited.
Telecom Namibia (2024)	The operator and regulator confirmed a ransomware-related incident and unauthorised data disclosure; public evidence of broad service outage was limited.	2	Confidentiality impact is clear; the cited sources do not document a service interruption sufficient for KSM=3.
CNSS, Morocco (2025)	Authorities confirmed cyberattacks and leakage of some social-security data, while warning that circulated documents included false, inaccurate or truncated material.	2	Serious confidentiality / trust event; large-scale operational outage is not established.

Incident	Documented consequence	Provisional KSM	KoI / evidence note
Government websites, Senegal (2023)	Multiple public websites were made unavailable through DDoS attacks; the event affected public information access rather than demonstrating compromise of underlying systems.	3	Confirmed availability effect; actor claims do not establish deeper compromise.

Figure 2. Illustrative cases 7–12.

5.1 Operational Disruption Reaching Physical or Clinical Processes

The Transnet and NHLS incidents show most clearly why KSM has to be tied to realised operations. In July 2021 South African government reporting stated that Transnet had restored full port operations after an IT security breach, allowing the national supply-chain and logistics system to return to normal (Government of South Africa, 2021). What matters analytically is not the ransomware label but the move from digital compromise to real-world container and port processes. The shift to manual operation, and the declaration of force majeure, show that the event crossed from information-system availability into physical logistics. A provisional KSM=5 is consistent with the scale's top level, while the KoI stays incomplete because the public sources do not establish all four technical behaviours.

5.2 Healthcare Dependency and the Difference Between Data and Care

The 2024 National Health Laboratory Service incident is a second case of realised operational consequence. The NHLS annual report describes a ransomware breach that severely affected IT systems and put the continuity of diagnostic services at risk (National Health Laboratory Service, 2025). A peer-reviewed account in the South African Medical Journal reports that affected files and servers became inaccessible and that laboratory operations, and stakeholders across the service, were disrupted (Cassim & Chapanduka, 2024). The consequence that counts here was not simply loss of data confidentiality. Laboratory orders, sample processing and result distribution are part of clinical decision-making, and when they become unavailable a cyber incident can affect patient care even without any direct manipulation of a medical device (Besenyő & Kovács, 2023). This supports a provisional KSM=5, with the KoI components left unscored where public forensic evidence is missing.

5.3 Sustained Public-Service Disruption Without Physical-Process Evidence

The South African Department of Justice incident sits one level lower. Departmental annual reporting describes ransomware that affected operations, and a statutory implementation report records a complete shutdown of departmental IT systems, including the Integrated Case Management System for Child Justice, lasting four months (South African Department of Justice and Constitutional Development, 2022). The duration and scope justify a high damage placement. The documented consequence, though, concerns the availability and administration of justice services rather than any

confirmed manipulation of a physical process. KSM=4 keeps the line between a sustained, system-wide service interruption and the physical-operational top category.

5.4 Response Capacity as Context Rather than Damage Inflation

The Western Cape Provincial Parliament case shows why organisational response should not be mistaken for attack severity. The institution's 2023 report states that ransomware left all servers inoperable, while its public communication stressed that parliamentary business carried on (Western Cape Provincial Parliament, 2023). The incident caused a real technical outage, but continuity arrangements held down the functional consequence, and a provisional KSM=3 captures that bounded disruption. A strong response does not mean the attack was trivial; it means recovery capacity limited how far the attack reached operationally. The quality of that response belongs in the context layer, not in a retrospective redefinition of the technical event.

5.5 Electricity Vending: Operational Importance Without Proven Grid Manipulation

The Electricity Company of Ghana case calls for the same restraint in the other direction. ECG later confirmed a ransomware event and reported that it could not vend prepaid electricity for about a week, with losses put in the hundreds of millions of Ghanaian cedis (Electricity Company of Ghana, 2024). Prepaid vending is central to revenue collection and to customer access, but the public account does not establish any direct manipulation of grid control, or a physical electricity outage caused by the attack. A provisional KSM=4 says more than treating the event as an administrative inconvenience, yet stays more defensible than a KSM=5 assigned on sector importance alone.

5.6 Availability Attacks on Core Digital Government Services

Kenya's eCitizen incident and Senegal's government-website incident illustrate availability harm with no evidence of deeper system compromise. Kenyan public statements described a DDoS attack that caused downtime and reported that services returned without a confirmed data breach (Citizen Digital, 2023). Reuters reported that several Senegalese government websites were made unavailable by DDoS attacks (Reuters, 2023). In both, KSM=3 is a reasonable illustration: public access to government information or services was disrupted, but the evidence does not show destruction of core records, sustained internal system loss or physical-operational effect. Both cases also show why a DDoS claim should not be stretched into an intrusion claim without evidence.

5.7 Third-party Concentration in Mobile-Money Ecosystems

The Uganda incident matters analytically because the affected object was an integration layer. According to MTN Uganda, the security breach occurred at Pegasus Technologies rather than in the operator's own core systems, and it affected the bank-to-wallet transfer channel; everyday services, from cash deposits and withdrawals to transfers between individual users and merchant payments, continued to operate (MTN Uganda,

2020). The case should not, then, be described as a total failure of mobile money. Its significance lies in the concentration of dependency: a third-party aggregator carried disruption across financial and telecommunications relationships even as the core platform stayed available. KSM=3 captures the affected transaction path, while functional criticality records why even a bounded integration failure can matter to users and institutions.

5.8 Central Banks: Partial Application Disruption Versus National Payment Interruption

The Bank of Zambia and Central Bank of Lesotho cases show the value of differentiating by consequence within a single institutional category. The Bank of Zambia's annual report confirms a cybersecurity incident in 2022, and contemporaneous reporting of the bank's statements records that the incident disrupted the bureau de change monitoring system and the public website, which was down for part of several days, while core systems remained up (Bank of Zambia, 2023; News24, 2022). Under the anchors in Section 3.2 that is the documented loss of a public-facing function with core institutional functions continuing, which supports a provisional KSM=3. The Central Bank of Lesotho, by contrast, confirmed a cyber-security incident that affected systems, and official communications recorded disruption and the subsequent restoration of payment services (Central Bank of Lesotho, 2023). Here the consequence reached national payment infrastructure, supporting a provisional KSM=4. Describing both simply as 'central bank cyberattacks' would hide the operational difference between them.

5.9 Confidentiality Loss Versus Service Interruption

Telecom Namibia and Morocco's National Social Security Fund illustrate incidents dominated by confidentiality and trust. Telecom Namibia and the Communications Regulatory Authority of Namibia confirmed a ransomware-related event and data exposure (Communications Regulatory Authority of Namibia, 2024; Telecom Namibia, 2024). The cited sources confirm data compromise but do not document a service interruption sufficient to support KSM=3, so the provisional placement is KSM=2 rather than a level lifted simply because the target is a national operator. In Morocco the government confirmed attacks on the CNSS and the leakage of some data, while warning that the circulated materials included false, inaccurate or truncated documents (Government of Morocco, 2025). The Associated Press reported that the social-security agency acknowledged data theft and leakage (Associated Press, 2025). KSM=2 reflects the limited documented operational interruption, while the separate functional-criticality and confidentiality fields capture the scale of the identity, employment, salary, pension and insurance dependencies involved.

6. Cross-Case Analysis

6.1 Impact and Sector Importance

The cases support the framework's basic separation between impact and sector. Ports, laboratories, justice systems, electricity distributors and central banks are all socially important, yet their incidents did not produce the same consequences. Transnet and

NHLS reached real-world operational processes; the Department of Justice and the Central Bank of Lesotho suffered sustained service interruption; the Western Cape Provincial Parliament kept its business running despite serious server loss; the Bank of Zambia saw a bounded outage of its public website with core systems intact; and the CNSS suffered a major confidentiality event without comparable evidence of system-wide service loss. A framework that starts from sector labels would push most of these to the top of a single risk scale, whereas one that starts from documented consequence keeps the variation that matters.

None of this denies that criticality shapes harm; it only changes where that influence is recorded. Functional dependence, the availability of substitutes, geographic reach and concentration all explain why the same technical consequence can matter more in one setting than another. A one-day outage of a lightly used portal is not the same as a one-day outage of a payment platform that carries essential transactions. But writing dependence into the damage score would make cross-case comparison impossible. The answer is a two-step statement: first record what the incident did, through KSM, then record who and what depended on the affected function, through the criticality layer.

6.2 Sparse Reporting and the Risk of Under-Scoring Complexity

The twelve cases say far more about consequence than about intrusion path. Official statements are generally written to communicate restoration, continuity and reassurance, and they rarely publish dwell time, privilege escalation, credential access, internal movement, defence evasion or the sequence of technical stages. For most of these cases, then, a defensible KoI total simply cannot be formed. That is less a weakness of the index than a finding about the evidence environment itself.

A binary coding rule would introduce a predictable bias. Suppose persistence, lateral movement and evasion were each scored zero whenever a press release failed to mention them. Organisations with mature forensic disclosure would then appear to suffer more complex attacks, because they publish more detail, while institutions that disclose little would appear to face simple ones. The model would end up measuring reporting maturity rather than adversary behaviour. The three-state approach (present, absent, not assessable) prevents this conversion of silence into negative evidence. Complete-case KoI values can still be used where the record supports them, provided any comparison also reports how many components were assessable.

The same logic applies to attribution. A public claim by a group can help establish motive or campaign context, but it does not prove operational control, sponsorship or state responsibility, and country, language or infrastructure location must not stand in for actor identity. Nigeria-focused research has treated cybercrime as an evolving institutional, economic and policy problem rather than a national characteristic (Kovács, 2022a). Evidence-constrained attribution is more than cautious wording: it keeps the analysis clear of circular, and potentially stigmatising, inference.

6.3 Functional Criticality Beyond Utility Lists

The case set shows that criticality in Africa cannot be read off the traditional energy, water, transport and health categories alone. Work on water-sector cybersecurity shows

that disruption can spread through health, production and wider social pressures even when the initiating event is purely technical (Kovács, 2024c). eCitizen concentrates access to public services; the CNSS concentrates employment, pension, insurance and identity information; mobile-money integrations connect banks, operators, agents, merchants and households; and central-bank payment systems coordinate national financial settlement. What makes these functions critical is that the effects of unavailability or integrity failure spread across many dependent services, not that a foreign regulatory list happens to label them critical.

The African Union's digital strategy and data-policy framework link digital infrastructure, digital government, financial services, digital identity, cybersecurity and personal-data governance (African Union, 2020, 2024). This article carries that policy insight into incident analysis without touching KSM. Functional criticality can be set out through four questions: how many essential functions rely on the service; whether a practical non-digital or alternative route exists; whether the dependency is concentrated in a single provider or intermediary; and whether an integrity failure can spread through shared identity, payment or data interfaces. The Uganda case is a good example, since the core mobile-money platform stayed intact and yet a third-party connection still disrupted a meaningful transaction path.

6.4 Recovery Capacity as Context

Manual operation and substitute processes recur across the cases. Transnet moved to manual port processes; the Department of Justice faced prolonged system loss and administrative backlog; the Western Cape Provincial Parliament carried on parliamentary business despite inoperable servers; and the NHLS relied on alternative communication and processing arrangements during a clinically sensitive outage. These measures shape duration, backlog and safety, but they should not be used to score an attacker's sophistication or to erase the initial damage.

The distinction earns its keep operationally. A KSM finding tells leadership what class of consequence occurred; the recovery context tells them how quickly the organisation, and the society that depends on it, can absorb that consequence. Two incidents at the same KSM can call for very different investment, because one institution has manual fallback, distributed capacity and tested restoration while another has a single digital path and no workable alternative. The payoff is a clearer risk register, in which event severity, service criticality and resilience capacity stand as separate reasons for action.

6.5 Different Consequence Types, Different Responses

The cases also push back against treating every severe cyber event as the same problem. The CNSS and Telecom Namibia call for privacy, identity-protection, legal and trust responses, because confidentiality loss is at the centre. eCitizen and Senegal call for availability protection and DDoS resilience. The Bank of Zambia and the Western Cape Provincial Parliament call for application and infrastructure recovery. Transnet, NHLS and ECG call for continuity analysis tied to physical logistics, clinical workflow or customer access to electricity. The Central Bank of Lesotho calls for payment-system

resilience and sector coordination. A single, undifferentiated 'cyber severity' number would hide all of these response pathways.

KSM is best understood as one axis, not a complete risk judgement. KoI answers a separate question about observable execution; KrI and functional criticality explain societal role; and the evidence state governs how firmly any conclusion may be stated. Taken together, the fields make up an auditable incident card, and they can be read together, and acted on together, without being merged into a single number.

7. Operational and Policy Implications

For operators, the framework changes the first question after an incident from 'How sophisticated was the attacker?' to 'What is confirmed, what function is affected, and what is still unknown?' Asked in that order, it puts containment and continuity ahead of attribution. A port or laboratory does not need a confident actor label before it activates manual procedures, preserves evidence, isolates systems and coordinates with the organisations that depend on it. Nor should an institution announce that an attack was simple just because its public report shows no lateral movement or persistence.

For regulators, the framework makes cross-sector comparison less hostage to disclosure bias. Reporting templates can ask for separate fields for operational interruption, confidentiality or integrity effect, recovery time, scope of dependency, source confidence and coverage of technical detail. A regulator can then tell a low-KSM but high-confidentiality event apart from a high-KSM continuity event, or spot sectors where low KoI values only reflect low assessability. That is more informative than ranking institutions by incident counts or by unqualified severity labels.

For security operations and risk management, the incident card supports a proportionate response. KSM guides continuity and safety escalation; the KoI components guide how deep an investigation goes and where threat-hunting should focus; KrI and functional criticality identify the dependent services and stakeholders; and the evidence state decides whether the organisation is acting on a confirmed fact, a plausible hypothesis or an open gap. Where early actor probabilities are used, they should allow an abstention state and should never hold up basic defensive action. When predictions feed operational triage, calibration and class-sensitive metrics matter more than headline accuracy (Niculescu-Mizil & Caruana, 2005; Sokolova & Lapalme, 2009).

For research, the immediate contribution is comparability held in check. Shared definitions let knowledge accumulate, while explicit unknown states stop the appearance of precision from running ahead of the sources. Distributional tools such as Jensen–Shannon divergence can tell whether two observed samples differ, but the reading still depends on whether their language, source class and reporting process are comparable (Lin, 1991). And where human coders turn narrative evidence into ordinal or categorical variables, inter-rater agreement and label-noise analysis remain essential (Cohen, 1960; Frénay & Verleysen, 2014).

8. Limitations

The twelve incidents are purposive illustrations. They over-represent events that became public and that produced accessible official or high-quality reporting, and they cannot

estimate how frequent ransomware, DDoS, physical impact, particular actor types or sector exposure are across Africa. Countries and institutions with stronger disclosure practices are more visible in such a set, and accessibility in English remains uneven even where French-language and official national sources were consulted.

The provisional KSM placements are interpretations of public evidence, not final adjudicated labels from a completed African incident corpus. Several cases could shift within a narrow band if fuller technical or operational records came to light. KoI totals are withheld wherever the four components cannot be assessed. Functional criticality, too, involves contextual judgement, and should be documented openly rather than presented as an objective property of a country or a sector.

Finally, the coefficients and performance figures in Section 3 belong to the original MCED analysis (Kovács, 2026). They justify using the constructs as an empirical baseline, but they are not estimates for Africa. What this article claims is conceptual and analytical applicability, not a completed regional validation.

9. Conclusion

African cyber incidents are often read through the importance of the victim, the name of the malware, the claimed actor or the sheer scale of leaked data. Any of these can be relevant, but none can stand in for a structured account of consequence, behaviour, criticality and evidence. The twelve cases show what conflation costs in practice. Transnet and NHLS show digital compromise reaching physical logistics and clinical operations. The justice and payment-system incidents show sustained public-service disruption. eCitizen and Senegal show availability attacks with no evidence of deeper compromise. Uganda shows third-party concentration carrying impact across an otherwise functioning mobile-money ecosystem. Telecom Namibia and the CNSS show how confidentiality loss can be severe even when operational interruption is harder to establish.

The framework handles these differences by keeping the dimensions apart. KSM records the technical-operational damage that was realised. KoI records only observable complexity. KrI and functional criticality say why the affected function matters, without manufacturing severity. The evidence state stops missing detail from turning into false absence. Recovery capacity explains societal consequence without rewriting the event. The fields can be read together while staying analytically independent.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Disclosure statement

Besenyő János serves as Head of the Editorial Team of the Journal of Central and Eastern European African Studies. The authors declare no other competing interests.

Data availability statement

The Maryland Cyber Events Database underlying the original analysis is publicly available from the Center for International and Security Studies at Maryland

(https://cissm.umd.edu/cyber-events-database). All African incident sources examined in this article are publicly accessible at the URLs listed in the references.

Notes on contributors

Prof. Dr. Besenyő János, PhD, is Professor and Head of the Africa Research Institute at Óbuda University and a Visiting Professor at the Centre for Military Studies (CEMIS), Stellenbosch University. His research addresses African security and defence studies. (https://orcid.org/0000-0001-7198-9328)

Kovács Attila Máté conducts research at the Doctoral School on Safety and Security Sciences, Óbuda University, on evidence-based modelling of cyber threats to critical infrastructure, including incident severity, complexity and predictive analysis. (https://orcid.org/0000-0001-5088-5749)

References

African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. Retrieved October 10, 2026 from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

African Union. (2020). *The Digital Transformation Strategy for Africa (2020–2030)*. Retrieved October 10, 2026 from https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.pdf

African Union. (2024). *AU Data Policy Framework*. Retrieved October 10, 2026 from https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf

Associated Press. (2025). *Hackers breach Morocco's social security database in an unprecedented cyberattack*. Retrieved October 10, 2026 from https://apnews.com/article/753ce01484ceb8d1ec02459910285235

Bank of Zambia. (2023). *Annual report 2022*. Retrieved October 10, 2026 from https://www.boz.zm/Bank_of_Zambia_2022_Annual_Report.pdf

Besenyő, J., & Kovács, A. M. (2023). Healthcare cybersecurity threat context and mitigation opportunities. *Security Science Journal, 4*(1), 83–101. Retrieved October 10, 2026 from https://zagrebsecurityforum.com/articles-securitysciencejournal/id/4280

Cassim, S., & Chapanduka, Z. C. (2024). Cyberattack on the National Health Laboratory Service of South Africa: Implications, response and recommendations. *South African Medical Journal, 114*(12), Article e2549. https://doi.org/10.7196/SAMJ.2024.v114i12.2549

Center for International and Security Studies at Maryland. (n.d.-a). *Cyber Events Database*. Retrieved October 10, 2026 from https://cissm.umd.edu/cyber-events-database

Center for International and Security Studies at Maryland. (n.d.-b). *Cyber Events Database codebook*. Retrieved October 10, 2026 from

https://cissm.umd.edu/sites/default/files/2023-03/Cyber%20Events%20Database%20Codebook.pdf

Central Bank of Lesotho. (2023). *Cyber security incident (CBL) and related restoration statements*. Retrieved October 10, 2026 from https://centralbank.org.ls/wp-content/uploads/Cyber_Security_Incident_CBL.pdf

Citizen Digital. (2023). *Government says eCitizen services back online following DDoS-related downtime*. Retrieved October 10, 2026 from https://www.citizen.digital/news/govt-says-e-citizen-services-back-online-after-cyber-attack-scare-n324390

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement*, *20*(1), 37–46. https://doi.org/10.1177/001316446002000104

Communications Regulatory Authority of Namibia. (2024). *CRAN stresses vigilance following ransomware attack on Namibian telecommunication operator*. Retrieved October 10, 2026 from https://www.cran.na/download/media-release-cran-stresses-vigilance-following-ransomware-attack-on-namibian-telecommunication-operator-15-december-2024/

Electricity Company of Ghana. (2024). *ECG lost nearly GH¢500 million due to ransomware attack*. Retrieved October 10, 2026 from https://www.ecg.com.gh/index.php/fr/media-centre/news-events/ecg-lost-nearly-gh-500-million-due-to-ransomware-attack-managing-director-confirms

Frénay, B., & Verleysen, M. (2014). Classification in the presence of label noise: A survey. *IEEE Transactions on Neural Networks and Learning Systems*, *25*(5), 845–869. https://doi.org/10.1109/TNNLS.2013.2292894

Government of Morocco. (2025). *Morocco calls cyberattacks on state institutions criminal*. Retrieved October 10, 2026 from https://maroc.ma/en/news/morocco-calls-cyberattacks-state-institutions-criminal-links-timing-us-sahara-stance

Government of South Africa. (2021). *Minister Pravin Gordhan commends Transnet for restoring full ports operations*. Retrieved October 10, 2026 from https://www.gov.za/news/media-statements/minister-pravin-gordhan-commends-transnet-restoring-full-ports-operations-29

GSMA. (2024). *The mobile economy Sub-Saharan Africa 2024*. Retrieved October 10, 2026 from https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf

GSMA. (2026). *The state of the industry report on mobile money 2026*. Retrieved October 10, 2026 from https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/the-state-of-the-industry-report-on-mobile-money-2026/

International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th ed.). Retrieved October 10, 2026 from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

INTERPOL. (2025). *Africa cyberthreat assessment report 2025*. Retrieved October 10, 2026 from https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf

Kovács, A. M. (2022a). Here there be dragons: Evolution, potentials and mitigation opportunities of cybercrime in Nigeria: A review, analysis, and evaluation. *Journal of*

Central and Eastern European African Studies, *2*(1), 68–81. https://doi.org/10.59569/jceeas.2022.2.1.55

Kovács, A. M. (2022b). Ransomware: A comprehensive study of the exponentially increasing cybersecurity threat. *Insights into Regional Development*, *4*(2), 96–104. https://doi.org/10.9770/IRD.2022.4.2(8)

Kovács, A. M. (2024a). Creating cyber resiliency in critical infrastructures. In *Critical infrastructure protection in the light of the armed conflicts* (pp. 247–256). Springer. https://doi.org/10.1007/978-3-031-47990-8_22

Kovács, A. M. (2024b). Evolving cybersecurity strategies: Analyzing trends in critical infrastructure attacks and defense mechanisms. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(4), 2941–2952. https://ijisae.org/index.php/IJISAE/article/view/6779

Kovács, A. M. (2024c). Migration perspectives of water sector cybersecurity. *Journal of Environmental & Earth Sciences*, *6*(3), 217–232. https://doi.org/10.30564/jees.v6i3.7020

Kovács, A. M. (2026). *Kiberbiztonsági fenyegetések hatékony előrejelzése a kritikus infrastruktúrák védelmében* [Effective prediction of cybersecurity threats in the protection of critical infrastructures]. Óbuda University. Retrieved October 10, 2026 from https://oda.uni-obuda.hu/handle/20.500.14044/37968

Lin, J. (1991). Divergence measures based on the Shannon entropy. *IEEE Transactions on Information Theory*, *37*(1), 145–151. https://doi.org/10.1109/18.61115

MITRE. (n.d.). *ATT&CK enterprise tactics*. Retrieved October 10, 2026 from https://attack.mitre.org/tactics/enterprise/

MTN Uganda. (2020). *MTN clarifies on the incident related to its mobile money services*. Retrieved October 10, 2026 from https://www.mtn.co.ug/mtn-clarifies-on-the-incident-related-to-its-mobile-money-services/

National Health Laboratory Service. (2025). *Annual Report 2024/2025*. Retrieved October 10, 2026 from https://www.nhls.ac.za/wp-content/uploads/2025/10/NHLS_Annual_Report_2024-2025.pdf

News24. (2022). *Zambian central bank refuses to pay ransom to hackers*. Retrieved October 10, 2026 from https://www.news24.com/business/economy/zambian-central-bank-refuses-to-pay-ransom-to-hackers-20220519

Niculescu-Mizil, A., & Caruana, R. (2005). Predicting good probabilities with supervised learning. In *Proceedings of the 22nd International Conference on Machine Learning* (pp. 625–632). https://doi.org/10.1145/1102351.1102430

Reuters. (2023). *Senegalese government websites hit with cyberattack*. Retrieved October 10, 2026 from https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing & Management*, *45*(4), 427–437. https://doi.org/10.1016/j.ipm.2009.03.002

South African Department of Justice and Constitutional Development. (2022). *2021/2022 inter-departmental annual reports on the implementation of the Child Justice Act*. Retrieved October 10, 2026 from https://www.justice.gov.za/vg/cj/IND-ANR-2021-2022-ChildJusticeAct.pdf

Telecom Namibia. (2024). *Update on cybersecurity incident*. Retrieved October 10, 2026 from https://www.telecom.na/media-centre/816-update-on-cybersecurity-incident

Western Cape Provincial Parliament. (2023). *Secretary's report 2023*. Retrieved October 10, 2026 from https://www.wcpp.gov.za/sites/default/files/Secretary%27s%20Report%202023%20Web.pdf

World Bank. (2023). *Digital Africa: Technological transformation for jobs*. Retrieved October 10, 2026 from https://documents1.worldbank.org/curated/en/099041423154514338/pdf/P1701510f05e7a0db0bd5a0718bbee2b94d.pdf