Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i05.038

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Cyber Resilience Against Ransomware and Advanced Persistent Threats in Saudi Arabia's Critical National Infrastructure

Mohamed Shafraz Fareegul Nizam[1]*
[1]Independent Researcher

***Corresponding Author**
Mohamed Shafraz Fareegul Nizam
Independent Researcher

Article History
Received: 29.07.2026
Accepted: 23.09.2026
Published: 28.09.2026

Abstract: As energy, water, transport, telecommunications, healthcare, finance and government services migrate to cloud platforms, industrial internet connectivity, remote operations and data-driven automation, Saudi Arabia's critical national infrastructure is becoming more digitally integrated. The integration enhances operational capability, but also provides routes for ransomware and advanced persistent threats (APTs) to move from information technology to operational technology, disrupt essential services, manipulate trusted identities and exploit supplier relationships. This review integrates recent peer-reviewed evidence on cyber resilience against these threats and interprets it for the Saudi critical-infrastructure context. The choice of a structured integrative review is due to the evidence being across the fields of cyber resilience, ransomware, APT behaviour, industrial control systems, zero trust, situational awareness, risk governance and recovery engineering. The synthesis suggests that prevention alone cannot deliver resilient infrastructure. It calls for service-centric governance, separation of business and operational environments, identity-based access control, threat-informed monitoring, secure and tested recovery, supplier assurance, and continuous adaptation after exercises or incidents. Ransomware and APTs differ in speed and goals, but both take advantage of weak identity, lack of asset visibility, trusted administrative pathways, and poor recovery design. The paper therefore proposes a Critical Infrastructure Cyber-Resilience Loop that incorporates govern, anticipate, withstand, detect, contain, recover and adapt functions around minimum viable service delivery. The review provides a practical framework for Saudi operators and policymakers, and also highlights research gaps in OT-specific resilience measurement, cross-sector dependency modelling, recovery assurance, and empirical evaluation of national cybersecurity controls.

Keywords: Cyber resilience, ransomware, advanced persistent threats, Saudi Arabia, critical national infrastructure, operational technology, industrial control systems, zero trust, recovery engineering.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

1. INTRODUCTION

Critical national infrastructure (CNI) is increasingly reliant on tightly coupled digital and physical systems. Connected industrial control systems, enterprise identity services, remote maintenance, cloud analytics and third-party software are increasingly relied on for electricity generation, oil and gas operations, water treatment, transport control, telecommunications, financial services, healthcare and government platforms. This builds efficiency and observability but changes the consequences of cyber compromise: an intrusion

could affect data confidentiality, but also service continuity, safety, public confidence, and interdependent national functions. Research on industrial control systems details the long asset life cycles, deterministic processes, safety constraints, and legacy protocols that make the direct transplantation of typical information technology (IT) security controls into operational technology (OT) environments challenging (Bhamare *et al.,* 2020). Thus, the security of CNI should be measured not only by its perimeter protection, but also by its ability to continue to perform critical functions under attack. Cyber resilience contributes to that larger goal. It's about preparing for bad events, absorbing and containing disruption, restoring trustworthy operations, and adapting after incidents. Reviews of resilience frameworks show that the concept is wider than cybersecurity compliance as it connects protection with continuity, recovery, organisational learning and measurable operational results (Sepúlveda Estay *et al.,* 2020; Tzavara & Vassiliadis, 2024). Similarly, Hausken (2020) argues that resilience decisions involve trade-offs across prevention, response, recovery, and societal consequences. This logic has been generalised in recent surveys to cyber-physical systems, where a key aspect is graceful degradation and service preservation as physical processes cannot always be stopped safely (Segovia-Ferreira, *et al.,* 2024). The distinction is particularly pertinent for Saudi Arabia, where CNI modernisation is occurring against the backdrop of large-scale digital transformation and increasing convergence between enterprise and operational environments. Two classes of threats illustrate the limitations of prevention-centric strategies particularly well. Ransomware includes unauthorised access, privilege escalation, lateral movement, data theft, encryption, and extortion. Recent work has shown the growing importance of ransomware for cyber-physical systems and critical services (Benmalek, 2024). In contrast, APTs are typically targeted, persistent, multi-stage campaigns that aim to avoid detection, maintain access, and pursue strategic intelligence, disruption, or manipulation goals. Che Mat *et al.,* (2024) demonstrate that correlating multi-stage behaviour, rather than just individual alerts, is often necessary to reliably detect APTs. Quintero-Bonilla and Martin del Rey (2020) describe APTs as having coordinated attack stages. While ransomware operators and APT actors may have different goals, they are increasingly using similar techniques, including credential theft, living-off-the-land activity, abuse of remote services, command-and-control channels, and exploitation of trusted supply chains. Saudi-specific research findings support the importance of organisational readiness. Alharbi *et al.,* (2021) found that the damage incurred by Saudi enterprises is influenced by cybersecurity practices, whereas Alzubaidi (2021) found that cybersecurity awareness is continuously changing. Rawindaran *et al.,* (2023) also link cybersecurity maturity with governance, policy and workforce capability in a Saudi context. These studies do not measure national infrastructure resilience directly, but they indicate that technology alone is not enough if authority, competence, policy implementation and incident preparedness are weak. Thus, this review discusses how Saudi CNI operators can combine technical, operational and governance capabilities to prevent ransomware and APT activity from escalating to long-term national service disruption.

2. Purpose of the study

The objective of this paper is to critically synthesise the peer-reviewed evidence on cyber resilience to ransomware and advanced persistent threats and to translate the evidence into a Saudi CNI framework that links threat prevention, operational containment, trustworthy recovery, governance, and continuous learning. This study not only looks at malware classification, but also at resilience of essential services. It considers IT, OT, people, suppliers and recovery dependencies as one socio-technical system.

3. Objective of the Study

The review is driven by five objectives. First, it pinpoints the exploitation of CNI architectures and operational dependencies by ransomware and APT campaigns. Secondly, it measures resilience controls in governance, identity, segmentation, monitoring, response, and recovery. Third, it contrasts the varying resilience requirements posed by fast, disruptive ransomware and low-and-slow APT operations. Fourth, it considers how international evidence can be read for Saudi critical sectors without assuming direct transferability. Fifth, it provides a useful life-cycle framework and research agenda for measurable, service-level cyber resilience.

4. Research Questions

The review considers four questions: What are the greatest technical and organisational weaknesses that make critical infrastructure susceptible to ransomware and APT compromise? Which integrated capabilities best limit attack propagation and support minimum viable services? What are the differences in detection, containment and recovery for persistent targeted intrusion and ransomware? What are the main research, managerial and policy priorities to enhance cyber resilience in Saudi CNI?

5. METHODOLOGY OF THE REVIEW

For this topic, a structured integrative review was applied that integrates heterogeneous evidence from cybersecurity, industrial control,

resilience engineering, risk management, and organisational governance. A statistical meta-analysis is not possible because the literature consists of surveys, conceptual frameworks, empirical security evaluations, case-oriented reviews and architecture studies with incompatible outcomes. Integrative synthesis makes it possible to compare these forms systematically while maintaining the distinction between evidence of technical effectiveness and evidence of governance or resilience design.

The search was limited to peer-reviewed work primarily published from January 2020 to December 2025. Searches were performed in Scopus, Web of Science Core Collection, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and main publishers' databases. Search concepts were combined with Boolean expressions like (ransomware OR "advanced persistent threat" OR APT) AND ("critical infrastructure" OR "industrial control system" OR cyber-physical OR OT) AND ("cyber resilience" OR recovery OR continuity OR detection OR "zero trust" OR "situational awareness"). As a country context was to be included, governance, and awareness and enterprise evidence a Saudi Arabia term was added to the targeted searches. We also conducted backwards reference checking from recent systematic reviews to identify influential studies relevant to resilience mechanisms. Inclusion criteria included: studies published in English and in peer-reviewed journals; directly relevant to at least one of the six analytical domains: CNI or cyber-physical resilience; ransomware; APT behaviour or detection; IT/OT protection; identity and access; or response and recovery. Studies were excluded if they were focused only on consumer privacy, malware classification without operational implications, purely mathematical algorithms without infrastructure relevance, non-peer-reviewed commentary, vendor marketing, or attack descriptions without any defensible control or resilience insight. Because this is a critical integrative review and not a PRISMA claim of exhaustive enumeration, the paper does not invent database hit counts, duplicate-removal totals, or screening numbers that were not independently recorded. The quality was assessed against the criteria of clarity of research purpose, transparency of method, evidential basis, relevance to CNI, and transferability to the Saudi operational context. Converging patterns were established in review papers, and empirical evaluations were given more weight when testing detection or control performance. For example, Karantzas and Patsakis (2021) provide empirical evidence on endpoint detection and response against Advanced Persistent Threat (APT) vectors. In contrast, comprehensive reviews such as the ones by Alhidaifi *et al.,* (2024) and Aghazadeh Ardebili *et al.,* (2024) are useful to map resilience strategies and risk assessment approaches. Evidence was assessed thematically instead of being reduced to a single number of quality as this would suggest comparability that the underlying approaches do not support. Synthesis was carried out in three stages. Evidence was coded for threat progression: access, persistence, privilege escalation, lateral movement, command and control, impact, and remediation. Second, controls were mapped to resilience functions: govern, anticipate, withstand, detect, contain, recover and adapt. Third, the resulting patterns were interpreted for Saudi CNI considering the OT constraints, high-availability requirements, supplier dependencies, and the need to maintain safe physical processes. This evidence-to-framework pathway is summarised in Figure 1. Table 1 then differentiates the resilience demands of ransomware and APTs so that common controls are not confused with identical operational responses.

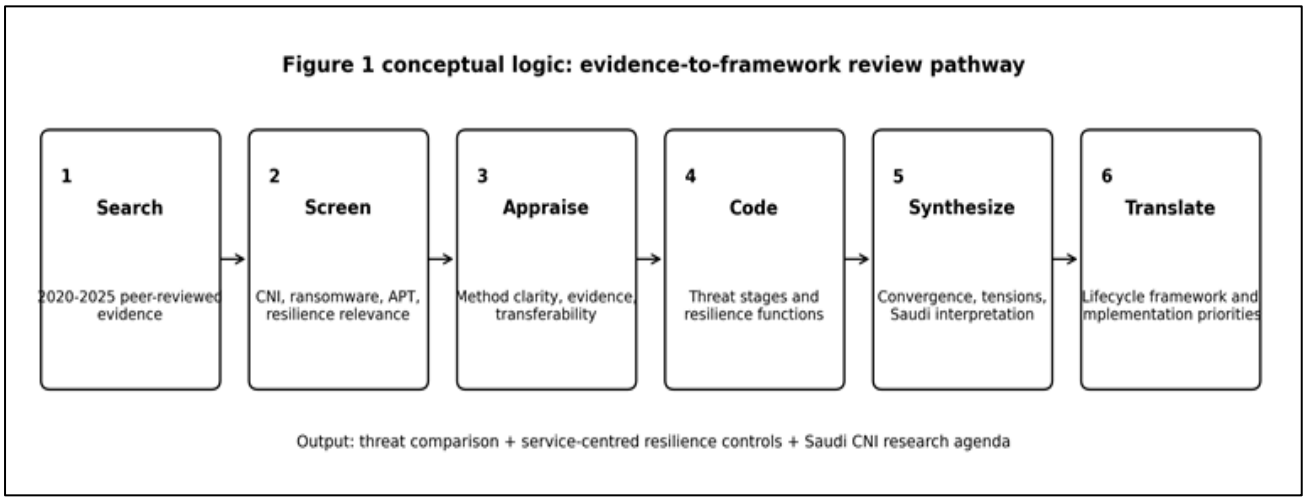

Figure 1: Evidence-to-framework review pathway used for the structured integrative synthesis

Table 1: Comparative resilience demands of ransomware and APTs in critical infrastructure

Dimension	Ransomware emphasis	APT emphasis	Shared resilience requirement
Operational tempo	Rapid escalation; visible service disruption	Long dwell time; stealthy progression	Predefined authority and service priorities
Primary concern	Encryption, extortion, data theft, recovery sabotage	Persistence, espionage, lateral movement, strategic manipulation	Identity control and propagation limits
Detection focus	Behavioral changes, privilege spikes, backup tampering	Cross-stage correlation, beaconing, persistence, anomalous administration	High-integrity multi-source telemetry
Containment	Fast isolation with business triage	Evidence-preserving, scoped eradication and hunting	Safe IT/OT segmentation and controlled access
Recovery	Immutable backups and rehearsed restoration	Confidence that restored systems and identities are clean	Trusted minimum viable service and isolated recovery

6. Critical Analysis And Thematic Literature Review

6.1. Ransomware and APTs:

Converging Resilience Issues Ransomware and APTs are often discussed separately, but CNI defenders gain from considering their shared enabling conditions. Ransomware research has evolved from file encryption signatures to behavioural detection, dynamic analysis and multi-stage mitigation. Dynamic and machine learning methods can identify ransomware behaviour but are sensitive to dataset quality, evasion and generalisation (Urooj *et al.,* 2022). In the same way, Kapoor *et al.,* (2022) highlight that detection should be combined with avoidance and mitigation, rather than viewed as a complete solution. Benmalek (2024) generalises the problem to the cyber-physical systems, where the encryption or the IT outage may affect the supervision, engineering workstations, maintenance systems, and operational decision support, even if the core controllers are not directly encrypted. APT research suggests persistence, stealth, and cross-stage correlation. Tatam *et al.,* (2021) show that threat modelling for APT-style attacks needs to model attacker progression rather than isolated vulnerabilities. Also, Zou *et al.,* (2020) propose detection based on evolving campaign behaviour. Finally, beaconing is particularly important because command-and-control traffic can be indicative of ongoing adversary presence following initial compromise. Abu Talib *et al.,* (2022) review methods for identifying such behaviour, remarking on variability in data and assumptions used for detection. Che Mat *et al.,* (2024) find that the combination of multi-stage behaviour and vulnerability context can improve the detection of possible attack paths.

The main takeaway is that ransomware is an acute resilience test and APTs are a chronic one. Ransomware needs fast containment, clean recovery and business prioritisation amid visible disruption. APTs require continuous telemetry, credential hygiene, threat hunting, provenance, and confidence that a system that appears to be restored is not still compromised. A CNI operator with great backups, but poor identity monitoring can recover from commodity ransomware, but still be vulnerable to persistent access. In contrast, an advanced detection programme with unverified restoration dependencies may detect an APT but still fail if destructive actions are taken. Therefore, resilience involves a simultaneous emphasis on persistence and recoverability.

6.2 IT/OT architecture, segmentation, and blast radius control

Critical infrastructure is different from normal enterprise IT in that availability and safety can limit patching, authentication changes, scanning and automated isolation. Legacy systems, specialised protocols, and physical-process consequences are long-standing industrial-control problems (Bhamare *et al.,* 2020). Thus, cyber-physical resilience research deals with graceful degradation and controlled operation rather than binary availability (Segovia-Ferreira *et al.,* 2024). Ahmadi-Assalemi *et al.,* (2020) also demonstrate that cyber resilience and incident response in smart environments are uneven, with research focusing more on detection, while other phases of response are less addressed. Saudi CNI architectural separation should decrease the number of trust paths over which compromise can travel from internet-facing services into operational zones. This does not mean absolute isolation, which is increasingly unrealistic, but it does mean explicit pipes, brokered administrative access, separate privileged identities, controlled remote maintenance and monitoring at the IT/OT boundaries. Cloud and IoT connectivity also create dependencies that need to be governed. Ahmad *et al.,* (2022) show that the IoT-cloud environments increase security exposure due to heterogeneous devices, interfaces, and data flows. Similarly, Parast *et al.,* (2022) recognise service-model and configuration risks that remain in cloud computing. The resilience implication is that

CNI architecture should be designed around failure containment: a compromised enterprise identity, software supplier or cloud workload should not automatically confer authority over safety-critical assets. Segmentation needs to be tested in operation. Static diagrams can be misleading about real reachability, since firewall rules, remote-access appliances, shared identity services, and temporary engineering exceptions change over time. Resilient operators therefore need asset inventories tied to communication paths and business services, and regular validation that high-consequence zones remain accessible only through intended means. The recovery infrastructure must be in a different failure domain as well. If production and backup administration are on the same identity plane, ransomware or an APT with privileged access can take them both down. The critical design question is not if segmentation exists on paper, but if an attacker who has compromised one zone can still gain credentials, routes, or management channels to access another.

6.3 Identity, Zero Trust and Supply Chain Trust

Identity has become a primary control plane for hybrid CNI environments as administrators, vendors, service accounts, applications, and automated tools routinely cross network boundaries. The zero-trust literature eschews implicit trust based on network location in favour of continuous verification, least privilege, and context-informed policy decisions. Teerakanok *et al.,* (2021) show that migration can be challenging when legacy systems cannot support modern identity controls, while Syed *et al.,* (2022) show that zero-trust architecture requires coordinated policy, identity, devices, data, applications and visibility rather than a single gateway. Moreover, Ramezanpour and Jagannath (2022) illustrate the importance of adaptive trust in software defined and next-generation network environments. Blast-radius reduction is the strongest near-term value of zero trust for CNI. Privileged access should be segregated from normal user accounts,-time bound, approved where practical and monitored. Disable vendor access by default and only enable during defined maintenance windows. Machine identities and service credentials need to be inventoried, rotated and scoped like human identities. Cao *et al.,* (2024) show that automation can improve zero-trust orchestration, but it also leads to interoperability, policy, and decision-risk problems. Automated denial or isolation in safety sensitive environments must be tested against operational consequences and must have controlled override processes. Trust also applies to software and suppliers. Collier and Sarkis (2021) suggest that zero-trust principles can be adapted to supply chains by replacing assumptions of permanent supplier trustworthiness with continuous verification. This is important for Saudi CNI, as specialised vendors may have remote access, proprietary software or engineering capability that operators cannot easily replace. Supplier assurance needs to cover access architecture, incident notification, evidence preservation, software provenance, recovery responsibilities, subcontractor transparency and exit planning. The goal is not to eliminate external dependency but to make dependency visible and recoverable.

6.4 Detection, Threat Correlation and Situation Awareness

To detect Resilient CNI you need to bring together endpoint, identity, network, application, cloud and OT telemetry. Karantzas and Patsakis (2021) found significant differences in endpoint detection and response capabilities against APT attack vectors, illustrating why product deployment alone does not guaranty coverage. Both Quintero-Bonilla and Martín del Rey (2020) and Che Mat *et al.,* (2024) argue that APT detection is improved when events are considered as stages of a campaign. In the case of ransomware, early containment can be achieved through monitoring dynamic behaviour such as unusual process creation, credential usage, bulk file operations, backup manipulation, or rapid privilege escalation, as opposed to relying on known malware signatures (Urooj *et al.,* 2022). But more telemetry doesn't necessarily mean better resilience. Logs require time synchronisation, asset context, integrity protection, retention and unambiguous ownership. A domain controller, safety engineering station or backup server should have a higher priority alert than a similar event on a low criticality asset. Research on situation awareness provides a useful bridge from detection to decision making. In the words of Bellini *et al.,* (2025), cyber-resilience situation awareness is not simply about collecting indicators, but about understanding the current conditions and anticipating likely developments. Salvi *et al.,* (2022) further illustrate how the digital-twin-oriented model can support common operational understanding in the electric-power ecosystem.

Detection engineering should therefore be service-centered for Saudi operators. Define high-value scenarios, determine what telemetry you need upfront, and then exercise your detections using credible ransomware and APT pathways. Threat hunting is especially important for APTs as persistence may be below normal alerting thresholds. Correlation of beaconing analysis, identity anomalies, anomalous administrative tooling, new persistence mechanisms, and divergence from known OT communication patterns can increase confidence. The goal is not maximum alert volume; it is timely

detection of attack progression with sufficient operational context to permit secure containment.

6.5 Recovery engineering, continuity and resilience measurement

Resilience is not traditional security. Recovery is the differentiator. Ransomware makes this obvious, because prevention can fail even in mature organisations, but APT actors might intentionally target backups, identity infrastructure, or recovery tooling before taking destructive action. Finally, Kapoor *et al.,* (2022) highlight that mitigation and recovery are as crucial as detection. Restoration and adaptation are invariably considered core capabilities in cyber-resilience surveys (Alhidaifi *et al.,* 2024; Tzavara & Vassiliadis, 2024). Recovery then must be designed as a reliable operational capability, not as a disaster-recovery plan that is seldom tested.

A CNI recovery design should identify minimum viable services and dependencies needed to restore them. Such dependencies include identity, naming, time services, keys, network routes, engineering repositories, databases, safety interfaces, telecommunications, supplier support, physical access, etc. Backups must be immutable or otherwise protected from production compromise, recovery credentials need to be isolated and restoration should be rehearsed under realistic conditions. The goal is not just file retrieval, it is to restore a trusted service state within acceptable recovery time and recovery point objectives while maintaining physical operations safe.

Measurement is still a problem. Cremer *et al.,* (2022) demonstrate that inconsistent loss data and heterogeneous measurement limit cyber-risk analysis. Aghazadeh Ardebili *et al.,* (2024) also observe a fractured landscape of resilience risk-assessment methods and standards. "Thus, useful measures for Saudi CNI should be based on observable service outcomes such as time to revoke compromised privilege, percentage of critical paths covered by telemetry, time to isolate a breached zone, proportion of critical services restored successfully in exercises, backup integrity pass rates, and unresolved supplier dependencies." The measures should be driven by service criticality, not aggregated into a single maturity score that may mask operational weaknesses.

7. DISCUSSION

The literature allows for a clear conclusion: ransomware and APT resilience is mainly an integration issue. Controls fail when governance, identity, architecture, detection, response, recovery and supplier management are owned as separate programmes and there is no shared service model. This helps explain why organisations can be compliant but operationally fragile. There is wide variation in resilience frameworks as identified by Sepúlveda Estay *et al.,* (2020) and resilience covers several technical and organisational domains as demonstrated by Alhidaifi *et al.,* (2024). The practical implication is that Saudi CNI operators should treat each critical service as an end-to-end resilience unit with an accountable owner, dependency map, threat scenarios, detection coverage, containment options, recovery objectives and exercise evidence.

The comparison of ransomware and APTs also shifts investment priorities. Ransomware resilience pays dividends in fast credential containment, segmentation, immutable backups, and rehearsed restoration. APT resilience rewards long horizon visibility, threat correlation, provenance, behaviour baselining, hunting, and confidence that recovery images and administrative systems are themselves clean. These priorities overlap, but they are not interchangeable. Undetected persistence won't be compensated for by a backup programme . Unrecoverable dependencies won't be compensated for by advanced monitoring . Thus the combination of detection confidence and recovery confidence is the strongest architecture. This results in the Critical Infrastructure Cyber-Resilience Loop depicted in Figure 2. Governance defines service criticality and accountability Anticipation uses threat intelligence, exposure analysis and scenario planning Withstand capabilities limit privilege and propagation Detection builds attack awareness Containment isolates unaffected zones and evidence Recovery rebuilds minimum viable services Adaptation translates lessons into design changes The loop corresponds with resilience research that views adaptation as an ongoing ability, rather than a return to a static pre-incident state (Hausken, 2020; Tzavara & Vassiliadis, 2024). Table 2 links this model to the Saudi CNI implementation priorities. Another implication concerns the link between assurance and resilience. For critical infrastructure, evidence of the existence of a control is weaker than evidence of performance under adversarial pressure. Access reviews may show that privileged accounts are documented but they don't show that emergency revocation works when identity services are degraded. Backup reports can show successful jobs, but they don't show that operators can piece together an interdependent service after credentials, configuration repositories, and management networks are compromised. Resilience assurance should include control testing, attack simulation, restoration exercises and decision-making drills. A good test starts with a believable scenario of attack, defines the minimum acceptable level of service, and asks whether people, technology, suppliers, and recovery resources can together deliver that result. This method translates abstract maturity into operational proof and helps uncover

hidden dependencies before an attacker can exploit them. Cross-sectoral coordination is important, as national infrastructure does not fall apart in organisational silos. Telecommunications support remote operation and emergency communications, electricity underpins almost all digital services, identity and cloud services may be shared across many organisations, and specialist suppliers can become common points of dependency. Thus, a ransomware outbreak or long-running campaign against one provider can have second-order effects elsewhere, even if downstream organisations are not directly compromised. Saudi resilience planning should incorporate dependency exercises where operators share only the information necessary to understand cascading impacts, while safeguarding sensitive technical detail. Such exercises can clarify escalation thresholds, alternate communications channels, restoration priorities and assumptions about external support. They also serve as a basis for comparing sector-level resilience without forcing organisations into a single technical architecture.

Lastly, governance has to explicitly acknowledge uncertainty. Threat intelligence will not predict every campaign. No control set will prevent compromise. Decision makers should therefore distinguish between known vulnerabilities, plausible attack paths, uncertain adversary capabilities and dependencies that have not yet been tested. Scenario planning can then prioritise investments by consequence and recoverability rather than by fear or technology fashion. This benefits capabilities that are useful across threat types: accurate asset ownership, constrained privilege, segmented administration, high-integrity telemetry, protected recovery, tested communications and clear authority when it counts. Cyber resilience is therefore not a replacement for prevention. It's the discipline that ties together prevention, response, continuity and learning when prevention is not complete. Those capabilities also provide a stable foundation for regulatory assurance and executive oversight with transparency.

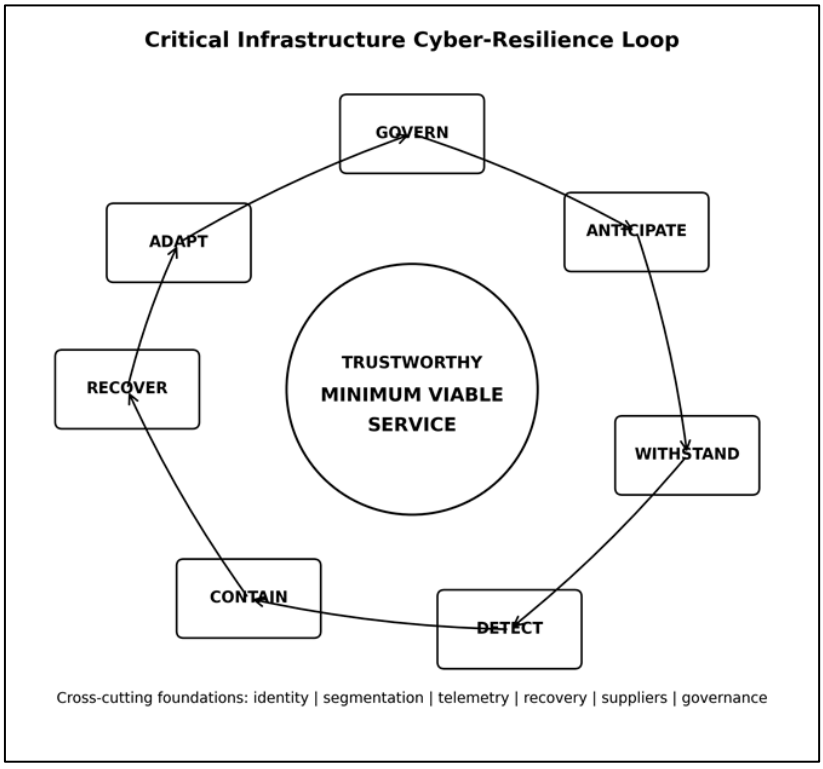

Figure 2: Critical Infrastructure Cyber-Resilience Loop for ransomware and APT resilience in Saudi CNI

Table 2: Saudi CNI implementation priorities mapped to resilience outcomes

Capability	Priority actions	Evidence of effectiveness	Resilience outcome
Govern and anticipate	Critical-service ownership; dependency mapping; scenario analysis; supplier accountability	Current service maps; exercised scenarios; accepted residual risks	Known exposure and decision authority
Withstand	Privileged-access separation; IT/OT segmentation; hardened remote access; secure configuration	Reachability tests; privilege coverage; exception closure	Reduced attack blast radius

Capability	Priority actions	Evidence of effectiveness	Resilience outcome
Detect and contain	Cross-domain telemetry; APT correlation; ransomware behavior analytics; safe isolation playbooks	Scenario detection tests; containment time; evidence preservation	Shorter dwell time and controlled impact
Recover	Immutable backups; isolated credentials; clean-room rebuild; minimum viable service sequencing	Successful restoration against RTO/RPO and integrity criteria	Trustworthy service restoration
Adapt	Post-incident learning; control validation; cross-sector exercises; supplier reassessment	Closed corrective actions; repeated exercise improvement	Continuous resilience improvement

8. Research Gaps and Future Research

Four gaps are of priority. First, empirical evidence specific for Saudi is still limited. National studies have addressed awareness and governance (Alharbi *et al.,* 2021; Alzubaidi, 2021; Rawindaran *et al.,* 2023), but peer-reviewed assessments of resilience controls in Saudi energy, water, transport, health and telecommunications settings are limited. Anonymized sector case studies and controlled exercises to measure service degradation, containment time and restoration performance should be included in future work.

Second, detection research is more advanced than recovery research. Ahmadi-Assalemi *et al.,* (2020) noticed that smart-city research is geared towards detection and analysis and a similar imbalance can be observed across CNI security. Studies should confirm that backup architectures, clean-room rebuilds, identity recovery, and OT fallback modes actually meet service objectives under ransomware and persistent compromise. Third, better modelling of interdependency is needed. Critical services depend on telecommunications, power, cloud platforms, identity providers, software vendors and specialist maintenance firms. Salvi *et al.,* (2022) show the utility of system representations such as digital twins, but more work is needed on cascading cyber effects across Saudi infrastructure sectors. Fourth, automated zero-trust and AI-assisted detection demand safety-aware validation. Cao *et al.,* (2024) mention orchestration challenges, and future studies should evaluate false positives, adversarial manipulation, operator override, explainability, and the consequences of automated isolation in OT. Longitudinal research linking control maturity to incident severity, downtime, recovery costs and safety impact would greatly strengthen the evidence base.

9. Implications for Practice, Management, and Policy

Practitioners should focus on organising resilience around critical services not security products. For each service you should identify a business owner and a technical owner, keep an up to date map of dependencies, privileged-access paths, required telemetry, containment procedures, minimum viable operating state, tested recovery sequence. Treat identity separation, controlled vendor access, IT/OT segmentation, protected backups and service-specific exercises as foundational capabilities. Cloud and IoT adoption should only happen with explicit understanding of shared responsibility and failure domains, in line with the risks described by Ahmad *et al.,* (2022) and Parast *et al.,* (2022). Operational results should be used to justify investments in resilience by managers. Boards and executives need proof about restoration confidence, unresolved single points of failure, supplier concentration, privileged-access coverage and exercise results, rather than counts of deployed tools. Ransomware and APT incidents cross organisational boundaries, so cybersecurity teams must collaborate with operations, engineering, continuity, procurement, legal, safety, and communications functions. Workforce development should focus on role-specific exercises and technical practice rather than just generic annual awareness.

The main implication for policymakers is that outcome-oriented assurance should complement control compliance. Critical operators should be encouraged to show that high-consequence services can be isolated, run in degraded mode where appropriate, and restored from trusted states. A sector-wide exercise can expose dependency failures that individual organisations cannot. Policy should also promote supplier transparency, coordinated incident reporting, interoperable evidence, and research partnerships that allow anonymized study of real incidents. Such measures would enhance national learning without requiring disclosure of sensitive operational detail.

10. CONSTRAINTS

This review has 4 limitations. It pools heterogeneous study designs and thus does not estimate a pooled effect size. The evidence base for Saudi CNI-specific operational outcomes is weaker than that for general cyber resilience, ransomware, and APT detection. The peer-reviewed literature in English may not capture relevant regional practice reported in Arabic or in confidential industry assessments. Finally, the review interprets published

evidence for the Saudi context but does not claim that international findings transfer without change across every sector, legacy platform or safety regime.

11. Summary

To achieve cyber resilience against ransomware and advanced persistent threats requires a paradigm shift from protecting individual assets to preserving essential services under compromise. The reviewed evidence shows that both threat classes leverage fragmented ownership, excessive privilege, weak segmentation, insufficient telemetry, supplier trust and untested recovery. They work differently. Ransomware compresses the decision time and directly tests restoration capability. APTs utilise patience, stealth, trusted access, and incomplete correlation. Thus, Saudi CNI requires defences that address both rapid disruption and long-term hidden presence. The proposed Critical Infrastructure Cyber-Resilience Loop integrates governance, anticipation, withstanding capability, detection, containment, recovery and adaptation around minimum viable service delivery. Its worth is in linking controls that are often managed separately. Identity policy must support segmentation; telemetry must reflect service criticality; containment must uphold safety; recovery environments must be decoupled from production compromise; and lessons from incidents and exercises must inform architecture and governance changes. Zero trust, advanced analytics and automation can strengthen this loop, but should be implemented with OT constraints and operational consequences in mind.

The most important next step for Saudi Arabia is evidence-based validation. Organisations should test whether critical services can be continued safely in degraded conditions, if privileged compromise can be contained, if persistent access can be detected and if services can be rebuilt from trusted states within realistic objectives. Instead of relying predominantly on maturity statements researchers should measure these capabilities across sectors and dependencies. A resilient national infrastructure isn't one where attacks never happen. It is one where compromise is contained, essential functions can be governed, recovery is reliable, and every incident makes the system that must face the next attack better.

REFERENCES

1. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. Applied Sciences, 14(24), 11807. https://doi.org/10.3390/app142411807
2. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics, 11(1), 16. https://doi.org/10.3390/electronics11010016
3. Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., & Maple, C. (2020). Cyber resilience and incident response in smart cities: A systematic literature review. Smart Cities, 3(3), 894-927. https://doi.org/10.3390/smartcities3030046
4. Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. Sensors, 21(20), 6901. https://doi.org/10.3390/s21206901
5. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. ACM Computing Surveys, 56(8), Article 196, 1-48. https://doi.org/10.1145/3649218
6. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016
7. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems, 4, 186-202. https://doi.org/10.1016/j.iotcps.2023.12.001
8. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security, 89, 101677. https://doi.org/10.1016/j.cose.2019.101677
9. Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of zero trust architecture: Potential solutions and challenges. Machine Intelligence Research, 21(2), 294-317. https://doi.org/10.1007/s11633-023-1456-2
10. Che Mat, N. I., Jamil, N., Yusoff, Y., & Mat Kiah, M. L. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. Journal of Cybersecurity, 10(1), tyad023. https://doi.org/10.1093/cybsec/tyad023
11. Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. International Journal of Production Research, 59(11), 3430-3445. https://doi.org/10.1080/00207543.2021.1884311
12. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3),

698-736. https://doi.org/10.1057/s41288-022-00266-6
13. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things, 11, 100204. https://doi.org/10.1016/j.iot.2020.100204
14. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. Sustainability, 14(1), 8. https://doi.org/10.3390/su14010008
15. Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), 387-421. https://doi.org/10.3390/jcp1030021
16. Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114, 102580. https://doi.org/10.1016/j.cose.2021.102580
17. Quintero-Bonilla, S., & Martín del Rey, A. (2020). A new proposal on the advanced persistent threat: A survey. Applied Sciences, 10(11), 3874. https://doi.org/10.3390/app10113874
18. Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. Computer Networks, 217, 109358. https://doi.org/10.1016/j.comnet.2022.109358
19. Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in Industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. Digital, 3(3), 200-231. https://doi.org/10.3390/digital3030014
20. Salvi, A., Spagnoletti, P., & Saad Noori, N. (2022). Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem. Computers & Security, 112, 102507. https://doi.org/10.1016/j.cose.2021.102507
21. Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A., & Garcia-Alfaro, J. (2024). A survey on cyber-resilience approaches for cyber-physical systems. ACM Computing Surveys, 56(8), Article 202. https://doi.org/10.1145/3652953
22. Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. Computers & Security, 97, 101996. https://doi.org/10.1016/j.cose.2020.101996
23. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679
24. Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. Heliyon, 7(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969
25. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to zero trust architecture: Reviews and challenges. Security and Communication Networks, 2021, 9947347. https://doi.org/10.1155/2021/9947347
26. Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. International Journal of Information Security, 23, 1695-1719. https://doi.org/10.1007/s10207-023-00811-x
27. Urooj, U., Al-Rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware detection using dynamic analysis and machine learning: A survey and research directions. Applied Sciences, 12(1), 172. https://doi.org/10.3390/app12010172
28. Zou, Q., Sun, X., Liu, P., & Singhal, A. (2020). An approach for detection of advanced persistent threat attacks. Computer, 53(12). https://doi.org/10.1109/MC.2020.3021548
29. Abu Talib, M., Nasir, Q., Bou Nassif, A., Mokhamed, T., Ahmed, N., & Mahfood, B. (2022). APT beaconing detection: A systematic review. Computers & Security, 122, 102875. https://doi.org/10.1016/j.cose.2022.102875
30. Bellini, E., D'Aniello, G., Flammini, F., & Gaeta, R. (2025). Situation awareness for cyber resilience: A review. International Journal of Critical Infrastructure Protection, 49, 100755. https://doi.org/10.1016/j.ijcip.2025.100755