Ingénierie des Systèmes d'Information
Vol. 31, No. 7, July, 2026, pp. 2435-2447
Journal homepage: http://iieta.org/journals/isi

A C4ISR-Integrated Framework for Critical Infrastructure Vulnerability Assessment in Nusantara Capital City

Agus H. S. Reksoprodjo

Asymmetric Warfare Study Program, Faculty of Defense Strategy, Universitas Pertahanan Republik Indonesia, Bogor 16810, Indonesia

Corresponding Author Email: yono.reksoprodjo@idu.ac.id

https://doi.org/10.18280/isi.310725

Received: 15 May 2026
Revised: 13 July 2026
Accepted: 22 July 2026
Available online: 31 July 2026

Keywords:
critical infrastructure protection, vulnerability assessment, C4ISR, smart city security, Nusantara Capital City, hybrid threats, defense planning

ABSTRACT

The development of Nusantara Capital City (IKN) as Indonesia's new administrative center introduces emerging security challenges associated with interconnected physical infrastructure, digital systems, and hybrid threats. Existing smart city security studies have rarely examined how defense-oriented situational awareness systems can be integrated with structured vulnerability assessment methods in a greenfield urban context. This study proposes a C4ISR-integrated framework combined with the Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER)+Shock methodology to support critical infrastructure vulnerability assessment and defense planning for IKN. A qualitative research approach was adopted through a structured review of 41 academic studies, policy documents, and institutional reports to identify major security concerns and assess critical assets. The assessment indicates that power and communication control systems represent the highest-risk components, with an overall risk score of 51/70, followed by transmission infrastructure at 50.5/70. The IKN Data Center is also identified as a priority asset because of its potential systemic impact on government and urban services. Based on these findings, the proposed framework integrates C4ISR-enabled situational awareness, vulnerability prioritization, and coordinated response mechanisms through an Integrated Command and Control Center (IC3). The study provides a conceptual foundation for early-stage security planning in smart capital cities and offers insights into protecting critical infrastructure in multidomain threat environments.

1. INTRODUCTION

1.1 Background: Nusantara Capital City as a national smart city

The relocation of Indonesia's capital city to Nusantara Capital City (IKN) in East Kalimantan, initiated under President Joko Widodo's administration (2014–2024), is far more than an administrative decision. It is a deliberate national mission to build a technologically advanced, digitally integrated city from the ground up, designed to serve as a model of equitable, sustainable, and future-ready urban governance [1]. Under this vision, every dimension of urban life, including public services, transportation, energy management, and environmental monitoring, is intended to be seamlessly connected through unified digital infrastructure, a commitment reaffirmed by the government as recently as 2025 [2, 3]. This greenfield character is IKN's greatest strategic asset. Unlike mature cities constrained by legacy systems, IKN can embed defense and security architectures into its planning from the outset. At the same time, however, this condition creates a distinctive vulnerability window: during active construction, incomplete systems, unresolved institutional arrangements, and evolving threat landscapes converge. The defense planning challenges addressed in this study are therefore not purely theoretical. They reflect real conditions on the ground at the time of writing. The framework proposed here is intended as a practical reference for policymakers currently shaping IKN's security architecture.

1.2 The urgency of modern defense planning for Nusantara

IKN's dual role as both the national seat of government and a strategic economic hub makes it a high-value target across multiple threat vectors. From a conventional military standpoint, threats may take irregular and asymmetric forms, including terrorism, sabotage, and deliberate infrastructure disruption. More significantly, the digital backbone of a smart city introduces acute exposure to cyberattacks and hybrid operations that combine physical and information-domain tactics [4, 5]. Addressing this challenge requires defense planning that goes well beyond perimeter security. It demands the integration of advanced command-and-control technologies, specifically C4ISR systems, with structured, evidence-based vulnerability assessment tools such as Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER)+Shock. Without this integrated approach, IKN's development trajectory will carry compounding security risks at every stage of construction and

eventual full operation.

1.3 Purpose and scope

This study investigates how a coherent smart defense planning framework can be developed for IKN through a systematic threat-anticipation methodology. Specifically, it aims to: (1) identify the conceptual integration gap between C4ISR systems and the CARVER+Shock methodology in the context of greenfield smart cities; (2) propose an operational framework that links military, civil, and digital domains; and (3) illustrate the framework's application through vulnerability scoring of IKN's critical assets, thereby generating actionable recommendations for policymakers, defense planners, and academics.

1.4 Novelty

A systematic review of the literature indicates that existing studies treat C4ISR architecture and the CARVER+Shock methodology separately, with no identified work operationalizing their integration within a unified smart defense framework for a greenfield capital city. CARVER+Shock, in particular, has been applied almost exclusively to conventional military targets and food-sector vulnerability assessments, where the target is assumed to be a fixed, already-built asset [6, 7]. This assumption represents the specific gap addressed in this study: existing CARVER+Shock applications assume a largely static target, and the methodology was not designed to accommodate an asset base that is still under construction and whose vulnerability profile shifts as C4ISR sensing capability comes online. The contribution of this study is a scoring approach that treats vulnerability as dynamically coupled with C4ISR maturity, rather than as a fixed property of the asset. This coupling, rather than the mere co-occurrence of two established tools, constitutes the specific analytical gap addressed in this study. The concurrent-design condition, rather than the greenfield label itself, is what makes this coupling observable in practice. Because IKN's C4ISR and physical infrastructure are being designed concurrently, the interaction between detection capability and vulnerability score can be built into the framework from the outset rather than added retroactively. Section 2.6 elaborates on how this combination has not yet been operationalized in existing work on smart cities and critical infrastructure protection.

2. LITERATURE REVIEW

2.1 The evolution of defense doctrine in developing countries

In developing countries, defense doctrine has shifted from a mainly military focus to a broader framework that also addresses non-military vulnerabilities and newer security threats, and Indonesia reflects this trend through repeated doctrinal revisions and a wider threat definition that includes social, economic, technological, disaster, and public-safety dimensions [8-10]. Prasetyo et al.'s [11] analysis of Indonesian defense doctrine highlights a broader pattern visible across developing nations: the gradual shift from conventional military-centric postures toward adaptive, multidimensional defense paradigms [12]. The study by Prasetyo et al. [11] is a policy-research repository publication rather than a peer-reviewed journal article. It is retained here because, to the author's knowledge, it is the most detailed available account of Indonesia's doctrinal evolution, and its central claim is corroborated by the peer-reviewed sources cited alongside it in this paragraph. This evolution is driven by globalization, rapid industrialization, and the proliferation of non-military threats, including cyber intrusions, economic coercion, and social disruption, that legacy defense frameworks were not designed to address. For a city such as IKN, which aspires to operate at the technological frontier, this doctrinal evolution is not merely relevant; it is a baseline requirement.

2.2 Smart defense models for smart cities

Smart cities present a dual-use challenge: the same integrated digital infrastructure that enables efficient urban governance also creates an extended and interconnected attack surface. Batty et al. [13] establish that future cities will rely on deep integration among information systems, sensor networks, and computational infrastructure for real-time urban management. Recent research on smart urban infrastructure further indicates that digital transformation introduces operational and information-technology risks that need to be incorporated into infrastructure risk assessment from the planning stage [14]. Taken together, these considerations show that security must be embedded as a design principle rather than appended as an afterthought, requiring defense architectures capable of operating across physical and digital dimensions simultaneously.

2.3 C4ISR as the backbone of modern defense

Fowler et al. [6]'s foundational work on network-centric warfare establishes C4ISR, or Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance, as the operational backbone of modern defense. C4ISR enables information integration and rapid coordinated response across land, maritime, air, and cyberspace domains [6, 15]. The MITRE Corporation has since standardized the C4ISR architecture framework as a reference model for defense system interoperability across allied nations [16]. More recently, advances in artificial intelligence and autonomous sensing have substantially expanded C4ISR's surveillance reach and accelerated its decision cycles, reinforcing its relevance for complex urban environments [15, 17]. The information-system requirements imposed by this interoperability, including data-schema alignment and control-system security, are established in Industrial Control System (ICS) security guidance such as NIST SP 800-82 [18, 19] and are discussed further in Section 5.5.

2.4 CARVER+Shock: From military origins to urban application

CARVER+Shock was developed by the U.S. Department of Defense as a structured tool for assessing the vulnerability of targets and assets. It evaluates seven dimensions: Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability, and Shock, the last referring to the broader psychological, social, and economic consequences of an attack [7]. The methodology was subsequently adopted by the U.S. Food and Drug Administration (FDA) for food-sector vulnerability assessments and has since been applied in peer-

reviewed studies examining supply-chain disruption and energy infrastructure risk prioritization, demonstrating its cross-domain transferability [7, 20, 21]. The present study extends this transferability further by adapting CARVER+Shock to evaluate critical urban infrastructure, an application for which no established precedent exists in the literature. The author has previously applied this methodology in national-level assessments, including discussions with Indonesia's State Intelligence Agency (BIN), where it proved effective for identifying protection priorities in sensitive infrastructure contexts [9]. This engagement is presented here as practitioner input that informed the study's scoring judgment, not as formal empirical validation of the methodology in an urban context. This distinction is discussed further in Section 3.4.

2.5 International best practices in smart defense

Two city-state cases offer instructive precedents. Tel Aviv has developed an integrated smart city ecosystem in which cybersecurity systems and urban infrastructure management operate through a unified data platform, supported by close collaboration among public agencies, private operators, and the technology sector [22, 23]. Singapore's Smart Nation provides a useful civilian-governance reference for understanding how digital infrastructure, data integration, and cross-agency coordination can support urban management. In this study, however, Singapore is treated as a contextual benchmark rather than as direct evidence of an integrated smart defense command-and-control model [24, 25]. Both cases suggest that successful smart defense depends on three interlocking conditions: technological integration, adaptive policy frameworks, and strong institutional collaboration. IKN must design all three conditions from the outset rather than retrofit them later. Two lessons from these cases directly inform the framework proposed in Section 4. From Tel Aviv, the unified data platform linking cybersecurity and infrastructure management informs the design of the Integrated Command and Control Center (IC3) in Section 5.4 as a single point of data fusion, rather than a coordinating body layered on top of separate systems. From Singapore, the cross-agency governance model informs the collaborative governance structure proposed in Section 5.2, in which institutional roles are defined before, rather than after, the technology is deployed. More recent peer-reviewed accounts of both cities' underlying technical infrastructure reinforce these lessons. Weinstein's account of Tel Aviv's Digi-Tel platform documents the data-integration and resident-facing service architecture behind the city's unified platform, while Das and Kwek's analysis of Singapore's pandemic-era digital tools documents the data-capturing sensors, geospatial mapping, and automated public-service systems that underpin its cross-agency data model [23, 25].

2.6 Identified literature gap

Prior contributions, including Prasetyo et al.'s [11] doctrinal analysis, Fowler et al.'s [6] C4ISR foundation, the FDA's CARVER+Shock validation, and the Tel Aviv and Singapore case studies, each make meaningful but partial contributions. None explicitly links or operationally integrates C4ISR and CARVER+Shock within a unified operational framework, and none applies such a framework to a greenfield capital city in a developing country. This gap is precisely what the present study addresses [6, 7, 11, 13, 22, 24].

This positioning requires direct comparison with an existing reference [26], the most closely related prior work published in the same journal, which proposes an integrated smart defense architecture for IKN [26]. This prior study establishes the case for architectural integration at the level of institutional design and command structure but treats the vulnerability assessment layer as a static input and does not couple it with the maturity of the C4ISR sensing layer. The present study's contribution relative to the prior study [26] is twofold: *first*, the dynamic coupling between C4ISR detection capability and CARVER+Shock sub-scores developed in Section 6.5; and *second*, the disaggregation of the Accessibility parameter into physical, cyber, and supply-chain vectors introduced in Section 7.3.

The positioning of the present study relative to prior literature, particularly in relation to C4ISR integration, CARVER+Shock application, and smart city defense planning, is summarized in Table 1.

Table 1. Positioning of the present study relative to prior contributions

Study	Focus	Method	Limitation	Contribution of the Present Study
Fowler et al. [6]	C4ISR	Conceptual	No urban integration	Integrates C4ISR with CARVER+Shock
FDA CARVER+Shock [7]	Vulnerability assessment	Applied	Non-urban context	Extends the method to smart city infrastructure
Smart city studies	Urban systems	Descriptive	No defense integration	Adds a defense architecture layer
Shiddiqy et al. [26]	Smart defense architecture for IKN	Conceptual and institutional design	Vulnerability is treated as static; no C4ISR–vulnerability coupling	Adds dynamic C4ISR-coupled scoring and Accessibility disaggregation

Note: C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; FDA = U.S. Food and Drug Administration; CARVER = Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability; IKN = Nusantara Capital City.

3. METHODOLOGY

3.1 Research design

This study is grounded in a qualitative approach that combines a structured literature review, policy document analysis, and conceptual mapping informed by practitioner-level insights derived from national security forums. Rather than relying on an unsystematic reading of available sources, the literature review was designed around a clear and transparent search and selection procedure, drawing on PRISMA-style reporting principles, so that the evidence base

underpinning the study can be traced and defended.

The search covered three main source repositories. Scopus was used to access indexed international peer-reviewed work; Google Scholar was used to broaden coverage to include grey literature and institutional reports; and SINTA/Garuda was used to capture Indonesian-language contributions that may not appear in international databases. Across these platforms, search strings were built around five thematic anchors: C4ISR, smart city security, critical infrastructure protection, CARVER+Shock, and IKN. These terms were combined with Boolean operators, and the search was limited to publications between 2000 and 2025 in either English or Indonesian. This initial search identified approximately 180 records.

The document set was then narrowed in several stages. First, titles and abstracts were screened to remove duplicates, sources without credible peer review or institutional backing, and pre-2000 works that could not reasonably be treated as foundational to current debates.

This step excluded 112 records and left 68 for closer examination. The remaining documents were read in full and assessed against the study's thematic focus. A further 27 records were excluded because they were only tangentially related to the research questions or did not provide sufficient methodological detail for synthesis. The 41 studies that passed all stages of assessment form the empirical and theoretical backbone of the analysis in this study. The overall selection process is summarized in a PRISMA-like flow diagram (see Figure 1), which traces the reduction from approximately 180 initial records to 41 studies included in the qualitative synthesis. The relationship between this literature base and the parameter scoring reported in Section 6 is made explicit in Section 3.3, where the scoring rationale for each CARVER+Shock dimension is traced to specific clusters of the reviewed literature.

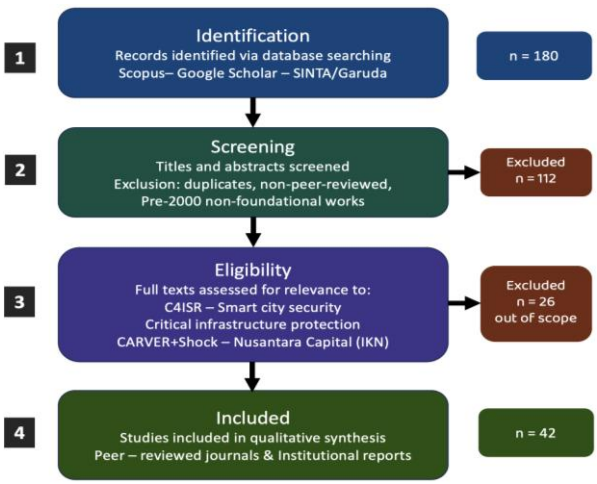

Figure 1. Structured literature review flow

3.2 Data sources

Data were drawn from several complementary sources. The first source consists of peer-reviewed academic literature from indexed international and national journals, with particular focus on C4ISR, smart city security, critical infrastructure protection, and the CARVER+Shock methodology. A second source consists of official policy documents, including IKN's Smart City Blueprint published by the Nusantara Capital City Authority (OIKN) and relevant national cybersecurity and defense regulations. The third source consists of international institutional references from NATO CCDCOE and the MITRE Corporation, along with documented experiences from Tel Aviv and Singapore. Finally, the analysis draws on practitioner insights gained through the author's participation in national strategic forums, including a formal presentation at the Coordinating Ministry for Political, Legal, and Security Affairs and technical discussions with the Research and Development Division of BIN [27].

This study also incorporates selected institutional and policy documents to capture real-time developments and regulatory contexts that are not yet fully reflected in the academic literature. Such sources are used selectively and primarily to complement, rather than replace, peer-reviewed evidence, particularly in areas where rapidly evolving policy environments, such as IKN development, limit the availability of indexed scholarly publications.

3.3 Analytical procedure

The analysis unfolded in three stages. It began by mapping the relevant literature on C4ISR and CARVER+Shock and identifying the issues that global debates have not yet addressed in relation to smart cities in developing countries. Building on this mapping, the study then translated the identified gap into a conceptual smart defense framework for IKN that links military, civilian, and digital domains and is deliberately designed to take advantage of IKN's greenfield status. Finally, the CARVER+Shock parameters were applied to IKN's main categories of critical assets, generating illustrative vulnerability scores that translate the framework into concrete prioritization guidance for security planners [28]. In this final stage, each CARVER+Shock parameter score was informed by a specific cluster of the reviewed literature. The Criticality and Effect scores drew primarily on studies of cascading infrastructure failure; the Accessibility and Vulnerability scores drew on smart city and physical security literature; and the Recognizability and Shock scores drew on social resilience and critical infrastructure studies. This mapping connects the qualitative synthesis of 41 studies to the scores reported in Table 2 and Table 3.

3.4 Validity and limitations

Analytical validity was strengthened through source triangulation, combining academic literature, government documents, and practitioner-derived insights. Given the cross-disciplinary nature of the subject, which spans technical, policy, and operational dimensions, no single source type provides a complete picture.

The principal limitation of the study lies in the illustrative character of the CARVER+Shock scores presented in Table 2 and Table 3. Because IKN's operational asset data are not yet publicly accessible for academic purposes, the scores reflect conceptual estimation. However, they are not arbitrary. The scores were derived through a single-analyst, literature-triangulated process: parameter calibration was benchmarked against established CARVER+Shock applications in critical infrastructure and food-sector risk assessment literature, and cross-checked against practitioner input obtained through engagement in national-level security discussions, including presentations to the Coordinating Ministry for Political, Legal, and Security Affairs and exchanges with the Research and Development Division of BIN [27]. This is explicitly not a formal multi-expert elicitation procedure, such as a Delphi

panel. It is a single-analyst judgment, cross-checked against the literature and practitioner discussion but not independently verified by a separate panel of raters. This is acknowledged here as a methodological limitation of the present study.

To enhance analytical consistency, cross-parameter validation was applied by comparing scoring patterns across asset categories, ensuring that assets with higher systemic interdependency consistently yielded higher Effect and Shock values. An informal robustness reflection was also conducted by re-examining whether the ranking of top-priority assets would change under moderate variation in individual parameter values. The ranking of the highest-priority assets did not change under this reflection, which provides a preliminary indication, not a statistical guarantee, that the prioritization order is not an artifact of any single parameter judgment.

Table 2. CARVER+Shock assessment of IKN critical assets

Critical Asset	C (Criticality)	A (Accessibility)	R (Recuperability)	V (Vulnerability)	E (Effect)	R (Recognizability)	Shock	Overall Risk Level (Indicative)
IKN Data Center	High (4)	Medium (3)	Low (1)	Very High (5)	Very High (5)	High (4)	High (4)	Very High (5)
Main power grid and communications	High (4)	Medium (3)	Medium (3)	Medium (3)	High (4)	Medium (3)	High (4)	High (4)
Clean water system	High (4)	Low (2)	Medium (3)	Medium (3)	High (4)	Medium (3)	Medium (3)	High (4)

Score legend: 1 = Low; 2 = Fair; 3 = Medium; 4 = High; 5 = Very High. Scale: 1 = lowest risk; 5 = highest risk.

Source: Author's assessment based on the CARVER+Shock framework [7].

Note: Scores are indicative and based on conceptual estimation calibrated with expert judgment; they are intended for prioritization illustration only. CARVER = Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability.

Table 3. CARVER+Shock assessment of the power grid, fuel distribution system, and communications subsector

Target	Criticality	Accessibility	Recuperability	Vulnerability	Effect	Recognizability	Shock	Overall	Rank
Fuel distribution system									
Gas pipeline	6.5	6	7.5	6.5	6	4.5	5.5	42.5	8
LNG	5.5	6.5	6.8	6.5	6.2	4.5	5.8	41.8	9
Power generation									
PLTG (Gas-Fired Power Plant)	6.5	6.5	6	6.5	6	4	5.5	41	10
PLTA (Hydroelectric Power Plant) and dam	7.5	5.5	7.5	6.5	7	7	7.5	48.5	4
Communications transmission system									
Towers and cable networks	8.5	8.5	6.5	8	7.5	5	6.5	50.5	2
Substations	8	7.5	6.5	7.5	7	4.5	6	47	6
Control Center, including ISO and RTO									
Facilities and personnel	9	6.5	6	7	8.5	5	7	49	3
Control systems	9.5	6	6	7.5	10	4.5	7.5	51	1
Distribution system									
Towers and cable networks	3.5	8.5	4.5	7.5	4	4	3.5	35.5	13
Underground lines	4	6	5.5	6.5	4.5	3.5	3.5	33.5	14
Transformers	5	7.5	4.5	7.5	5.5	4	4	38	12
Substations	6	7	5.5	7	6	4	4.5	40	11
Communications system									
Operational	8.5	6.5	6	7.5	8	5	6.5	48	5
Commercial, including trading	7.5	7	6	7.5	7.5	5	6	46.5	7

Score notes: Scale 1–10, where 1 = low risk or favorable condition, 5 = moderate risk, and 10 = high or critical risk.

Source: Author's assessment based on the CARVER+Shock framework [7].

Note: Scores are indicative and based on conceptual estimation calibrated with expert judgment; they are intended for prioritization illustration only. LNG = Liquefied Natural Gas; PLTG = Pembangkit Listrik Tenaga Gas, or gas-fired power plant; PLTA = Pembangkit Listrik Tenaga Air, or hydropower plant; ISO = Independent System Operator; RTO = Regional Transmission Organization; CARVER = Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability.

Accordingly, the scores are intended as a prioritization heuristic rather than an operationally definitive risk assessment, serving as a guide for sequencing protective measures pending empirical verification. This limitation also highlights a clear direction for future research: once IKN reaches operational status and data governance conditions permit, the framework can be applied with empirical precision [11].

The CARVER+Shock scales used in Table 2 (1–5) and Table 3 (1–10) differ intentionally. The first provides a strategic overview, while the second enables finer-grained prioritization within the energy and communications subsector. Internal consistency across asset classes was checked using this approach. The ranking of top-risk assets, namely Control Systems and Transmission Networks, did not change under moderate parameter variation, which is consistent with, though not proof of, a stable prioritization order.

3.5 Conceptual validation strategy

Due to restricted access to IKN's operational data, this study relies on a three-layered conceptual validation strategy. The first layer ensures theoretical consistency through the alignment of C4ISR and CARVER+Shock with established defense and infrastructure protection literature, while simultaneously evaluating how effectively these frameworks transfer to urban infrastructure environments. The second layer strengthens the process through scenario-based reasoning, which tests the framework against multidomain threats to ensure its internal coherence and operational plausibility. The third layer identifies the conditions under which empirical validation can be undertaken once operational data become available. Although empirical testing remains a future objective, this approach provides a defensible foundation for early-stage smart defense planning in a greenfield context.

4. CONCEPTUAL FRAMEWORK FOR SMART DEFENSE PLANNING

4.1 Principles of layered smart defense

Drawing on the author's presentation at the Coordinating Ministry for Political, Legal, and Security Affairs, smart defense planning for IKN must rest on a layered architecture that integrates hard defense, including military deterrence and physical security, with soft defense, including non-military resilience, civil protection, and diplomacy [11, 27]. This layered design must account for IKN's specific geographic character, the resilience requirements of its infrastructure, the need for interoperability across military branches, and the pace of technological change. It must therefore address conventional and digital threats simultaneously rather than sequentially.

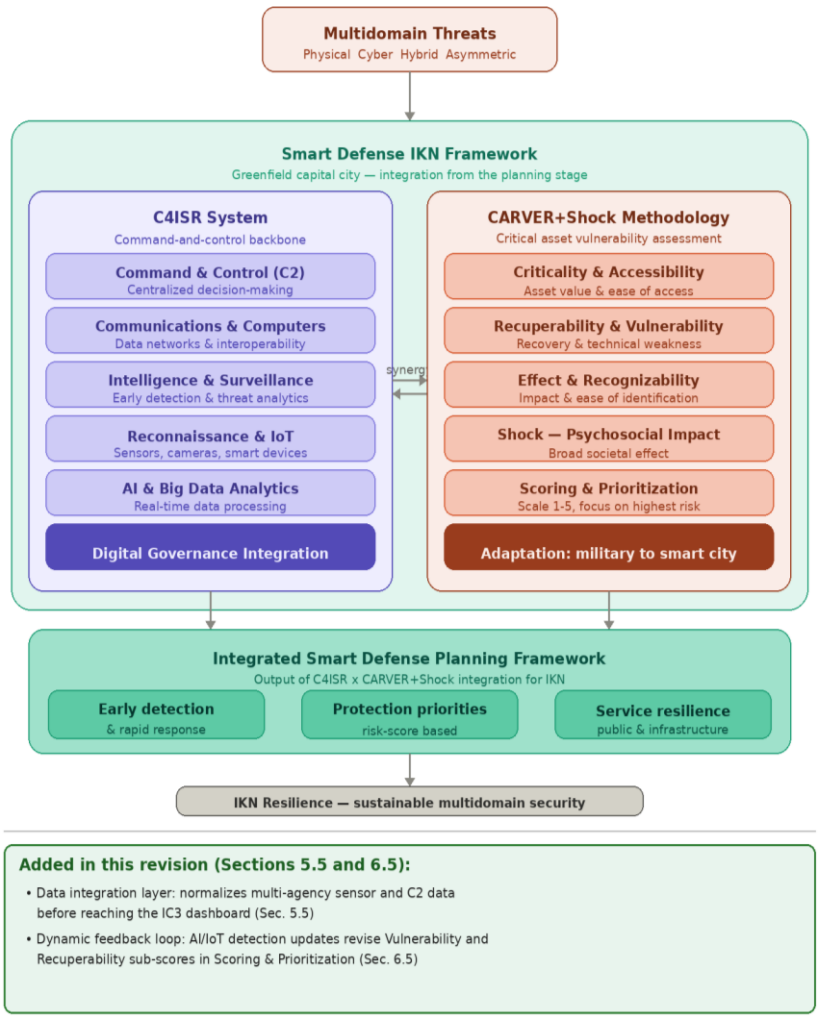

Figure 2. Integration framework of C4ISR and CARVER+Shock for IKN smart defense planning
Note: CARVER = Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability.

4.2 C4ISR, digital governance, and information technology synergy

Effective smart defense governance in IKN depends on a C4ISR system that is natively integrated with the city's digital governance infrastructure and information technology backbone. This integration enables surveillance, inter-agency communication, and command decision-making to occur rapidly and efficiently within a single operational picture. Crucially, this is not merely a defense objective: a well-implemented C4ISR layer directly supports responsive and transparent smart city governance, or smart government, by connecting security management to everyday urban operations and community welfare.

4.3 Critical asset identification and classification

IKN's critical assets span six primary categories: government administrative infrastructure, public service facilities, transportation networks, data centers, water and energy supply systems, and vital public spaces. Systematic identification and classification of these assets require a cross-agency inventory process that accounts not only for functional criticality but also for legal status, including land ownership validity, to ensure that protection planning is based on a reliable factual foundation [2].

4.4 Vulnerability assessment using CARVER+Shock

Every asset and system category in IKN warrants structured vulnerability evaluation. The CARVER+Shock framework provides this structure by scoring assets across seven parameters: Criticality, or the asset's importance to system function; Accessibility, or the ease of physical or cyber access by a threat actor; Recuperability, or the speed and cost of recovery after disruption; Vulnerability, or technical exposure to attack; Effect, or the magnitude of downstream consequences; Recognizability, or visibility and identifiability to potential attackers; and Shock, or the broader psychological, economic, and social effects of a successful attack, extending far beyond direct physical damage [7].

Scores across these dimensions generate a composite risk profile for each asset, enabling defense planners to prioritize resource allocation objectively by focusing protection on the assets for which a successful attack would cause the greatest cascading harm across IKN's multidomain environment [29].

Figure 2 illustrates the integrated C4ISR and CARVER+Shock planning framework developed in this study. The framework operates through three functional layers: situational awareness generation through C4ISR, structured vulnerability scoring using CARVER+Shock, and decision prioritization for resource allocation. These layers are interconnected through a continuous feedback loop in which real-time intelligence updates dynamically refine vulnerability assessment and response strategies.

5. SMART DEFENSE IMPLEMENTATION STRATEGY

5.1 AI, Internet of Things, and big data for early detection

The integration of artificial intelligence, Internet of Things (IoT) sensor networks, and big data analytics creates the technological foundation for real-time urban security monitoring. A distributed network of sensors, cameras, and smart devices deployed across transportation corridors, energy generation nodes, and public service facilities continuously feeds data into an analysis layer capable of detecting anomalous patterns [29, 30]. When anomalies cross predefined thresholds, the system automatically triggers early-warning protocols and generates response-option recommendations for command center operators, compressing the interval between threat recognition and coordinated action [31].

5.2 Cross-sector collaborative governance

Smart defense governance in IKN cannot be the preserve of any single institution. Effective operation requires structured collaboration among the Indonesian National Armed Forces (TNI), the National Police (POLRI), BIN, OIKN, digital infrastructure operators, and, where appropriate, community networks [32]. This collaboration must be codified in joint standard operating procedures with clearly assigned roles and escalation authorities, supported by a unified data platform that enables rapid, evidence-based decisions without the friction of inter-agency information silos or institutional rivalries [29]. This cross-agency imperative is reinforced by official policy discourse. Senior officials at the Coordinating Ministry for Political, Legal, and Security Affairs have articulated that IKN's defense architecture must rest on four interconnected pillars: universal defense, active deterrence, layered smart defense, and an anti-access/area-denial framework encompassing defense posture development, smart defense system establishment, and institutional capacity strengthening [33].

5.3 Risk mitigation for vital infrastructure

CARVER+Shock vulnerability scores provide the evidence base for designing differentiated risk mitigation measures across IKN's critical infrastructure sectors, including electricity, water, transportation, telecommunications, and data centers [30]. From these scores, planners can specify technical and organizational measures such as system redundancy configurations, layered physical and cybersecurity protocols, and service-continuity procedures designed to ensure that disruption at any single node does not cascade into city-wide failure [32].

5.4 Integrated Command and Control Center

An IC3 serves as the operational nerve center of IKN's smart defense architecture, consolidating data streams from the sensor network, C4ISR systems, and smart city management applications into a unified situational awareness picture [21]. Interoperability among these systems, achieved through a common network architecture and standardized application programming interfaces (APIs), allows operational information to flow with minimal latency across military units, security forces, city management authorities, and emergency services, thereby enabling simultaneous and coordinated responses to complex incidents [29], consistent with real-world integrated command architectures for capital-city air and homeland defense, such as Jakarta's command-and-control system [34].

5.5 Information system architecture of the Integrated Command and Control Center

The synergy between C4ISR and digital governance

described in Section 4.2 depends on a specific information system architecture, not merely on organizational coordination. At the sensor layer, distributed IoT devices, cameras, and monitoring equipment, as described in Section 5.1, generate raw telemetry that is transmitted to a data-integration layer. At this layer, inputs from multiple agencies, including TNI, POLRI, BIN, OIKN, and infrastructure operators, are normalized into a common data model before reaching the command dashboard used by IC3 operators. Interoperability across this pipeline requires standardized APIs and a common data-exchange format. Without these mechanisms, the unified situational awareness picture described in Section 5.4 collapses into a set of parallel, non-communicating systems, a known failure mode in ICS environments [18, 19]. This study does not specify the IC3 information architecture at the implementation level but recommends that its design be benchmarked against established ICS security guidance, particularly NIST SP 800-82 for control-system-specific threat vectors [18, 19, 35], and against the European Union's Network and Information Security (NIS) Directive for governance obligations applicable to operators of essential services [36]. Aligning the IC3 architecture with these established frameworks would address a structural gap in the present study. The C4ISR and CARVER+Shock components described in Sections 4 and 6 are integrated at the level of planning logic, but their integration at the level of data schemas, authentication protocols, and system interoperability requires further engineering specification beyond the scope of this conceptual study.

6. THREAT ANALYSIS AND RISK EVALUATION

6.1 Multidomain threat mapping

Threat mapping for IKN encompasses three principal domains: physical operations targeting vital infrastructure objects; cyber operations directed at the city's digital systems; and information or psychological operations conducted within a broader hybrid warfare framework [22]. This mapping exercise identifies not only the probable actor profiles and motivations behind each threat category, but also the specific attack vectors and cascading failure pathways through which a successful attack in one domain could degrade IKN's functions in others [2, 37].

6.2 CARVER+Shock vulnerability assessment

Applying CARVER+Shock to IKN's critical assets generates structured, comparable risk profiles across the asset portfolio. The methodology scores each asset across all seven dimensions, producing a total score that reflects overall risk exposure. Assets with the highest scores, particularly those combining high criticality and vulnerability with severe shock potential, constitute the priority tier for protective investment, consistent with comparative risk-assessment methodologies used elsewhere in cybersecurity practice [7].

Table 2 presents illustrative CARVER+Shock scores for three principal IKN asset categories using a 1–5 scale. Scores reflect conceptual estimation based on publicly available information and expert judgment; they are indicative rather than operationally definitive. All CARVER+Shock dimensions are treated with equal weighting in this study because operational prioritization data are not yet available. However, sensitivity to weighting variation is acknowledged as a limitation. As noted in Section 3.4, the Accessibility parameter, in particular, aggregates physical, cyber, and supply-chain access vectors into a single value. This simplification and its implications are discussed in Section 7.3.

The Shock rating for the IKN Data Center is scored at 4 rather than the maximum 5 because, while a successful attack would cause severe functional disruption, the psychological and social cascading effects are assessed as somewhat more contained than those of a total power-grid failure, which would be immediately visible and felt across the entire population. This distinction reflects CARVER+Shock's separation of systemic effect, captured under Effect, from broader societal panic and perception, captured under Shock.

The IKN Data Center emerges as the highest-priority asset: its combination of maximum Vulnerability and Effect scores with a very high Shock rating reflects the systemic consequences of a successful data-center compromise, which could potentially disable multiple government functions simultaneously. By contrast, the Clean Water System, while critically important, scores lower on Shock and Recognizability, suggesting a different protective posture that prioritizes resilience and redundancy over perimeter hardening.

6.3 Detailed subsector analysis: Power and communications

A finer-grained application of CARVER+Shock to IKN's power generation, transmission, distribution, and communications infrastructure uses a 1–10 scale to enable more nuanced differentiation. IKN's planning vision emphasizes low-carbon and renewable energy. In practice, however, the transition toward a fully renewable electricity system may still require interim assets to maintain supply reliability. For this reason, Table 3 includes gas pipelines, LNG facilities, and gas-fired power plants as transitional energy-security assets, not as permanent elements of IKN's long-term energy model.

The scoring indicates that the Control Center, specifically its Control Systems, ranks first with an overall score of 51, while Towers and Cable Networks in the Transmission subsystem rank second with an overall score of 50.5. Facilities and Personnel within the Control Center also rank highly, with an overall score of 49, reinforcing the need to secure both technical systems and human-operational components. A successful attack on the Control Systems could constitute a single point of failure capable of triggering cascading shutdowns across multiple infrastructure domains. The Control Systems assessed here are distinct from the Distribution subsystem's physical delivery assets in Table 3. Their Vulnerability sub-score reflects the specific exposures of the control layer. Although Control Systems and Distribution Towers and Cable Networks share a Vulnerability value of 7.5 and both fall within the broader power and communications subsectors, their priority ranking is determined by the total assessment, particularly their Effect and Criticality scores. These findings directly affect the prioritization of protective measures. The Control Center requires strengthened physical security, redundant command paths, and dedicated cyber defense protocols before any other asset category.

6.4 Incident response simulation

Vulnerability scoring must be complemented by scenario-based simulation exercises. Illustrative scenarios for IKN include coordinated disruption of the integrated power grid, a cyberattack on the Command and Control Center's operational systems, and a natural disaster that severs transportation access to critical government facilities [37]. Such exercises serve multiple functions: they reveal realistic response timelines, expose inter-agency coordination friction points, and identify procedural weaknesses that are not apparent in static risk assessments. Findings from simulation exercises should be systematically fed back into standard operating procedure updates, targeted retraining programs, and emergency system capacity enhancements, thereby creating a continuous improvement loop [17].

6.5 Effect of implementation on risk scores

Deployment of the AI/IoT detection layer described in Section 5.1 is expected to reduce the Vulnerability sub-score for Control Systems in Table 3 by improving early-warning lead time. However, it does not reduce the Criticality or Effect sub-scores, which reflect the asset's structural importance rather than the speed of threat detection. This distinction matters because the implementation measures proposed in Section 5 do not eliminate risk; they shift it. A Control System with a shorter detection lag is not a less critical asset, but it is less vulnerable in the specific sense that operators have more time to intervene before an anomaly becomes a failure. Framed in this way, the vulnerability assessment in Sections 6.2 and 6.3 and the implementation strategy in Section 5 are not two independent components of the study. Rather, the latter is intended to act on specific sub-scores of the former. Future applications of this framework should re-score Vulnerability and Recuperability once the AI/IoT detection layer becomes operational, to confirm whether the anticipated reduction is observed in practice.

7. DISCUSSION

7.1 The strategic value of greenfield integration

The findings of this study point to one particularly significant implication: the optimal moment to build security into a city is before the city fully exists. IKN's greenfield character is not merely a logistical convenience; it is a strategic asset that existing smart city frameworks have largely overlooked. Tel Aviv and Singapore both achieved high levels of smart defense integration, but they did so through the incremental retrofitting of security systems onto pre-existing urban fabrics [22, 24]. IKN can, in principle, achieve a higher degree of architectural coherence by designing C4ISR connectivity, sensor infrastructure, and redundancy mechanisms into its physical and digital layout from the outset. The integrated framework proposed here is structured to realize this advantage.

7.2 Limitations and conditions for full implementation

Implementing this framework at full operational fidelity depends on resolving gaps that currently exist outside the academic domain. The most pressing is data access: the CARVER+Shock scores in Table 2 and Table 3 are calibrated estimates, not field measurements, and they will need to be replaced with classified asset assessments once IKN reaches operational status. This limitation is not a flaw in the framework; rather, it is a consequence of the greenfield condition. A more structurally difficult issue is the regulatory gap. Indonesia's existing defense and security legislation does not yet define clear command authority among TNI, POLRI, BIN, and OIKN in a joint smart defense context. Without a legal foundation, the inter-agency coordination described in Section 5.2 remains aspirational. The final constraint is institutional: operating C4ISR systems and conducting CARVER+Shock assessments require a specialist workforce that does not yet exist at scale in Indonesia's defense sector. A technically sound framework operated by an underprepared workforce will not deliver its full potential.

7.3 Theoretical contribution

The theoretical significance of this study lies not in demonstrating that CARVER+Shock can be transplanted to a new domain, but in identifying a specific modification that the methodology requires when applied to a cyber-physical urban context. This study proposes disaggregating the Accessibility parameter for cyber-physical urban infrastructure into three vector-specific components: physical accessibility, cyber accessibility, and supply-chain accessibility. These components can be aggregated into a weighted composite score rather than reported as a single undifferentiated value, as discussed in Section 3.4 and Section 6.2 and illustrated in Table 4. This modification directly addresses a structural limitation of the original CARVER+Shock methodology when applied beyond single-vector physical targets. It therefore constitutes the study's principal theoretical contribution, rather than merely confirming that the tool's underlying logic holds in a new setting. The proposed integration model, which pairs C4ISR architecture with CARVER+Shock in a greenfield planning context, is not IKN-specific. Countries building new administrative centers or expanding capital functions into underdeveloped regions face structurally similar problems. The broader implication for defense planning scholarship is that frameworks developed for NATO conditions or high-income East Asian contexts may require substantial recalibration before they can be applied to countries where regulatory infrastructure, institutional capacity, and technology access differ significantly.

To make this disaggregation concrete rather than purely conceptual, Table 4 applies it to the three highest-ranked assets identified in Table 3 and Section 6.3. The physical, cyber, and supply-chain component scores are illustrative expert judgments consistent with the single-analyst procedure described in Section 3.4. The weights reflect the relative dominance of each access vector for each asset type. For example, transmission towers are physically exposed in open terrain and are therefore weighted more heavily on the physical vector, whereas Control Systems are reached predominantly through network access and are therefore weighted more heavily on the cyber vector. The weighted composite reproduces, within rounding, the single Accessibility value already reported in Table 3, confirming that the disaggregation refines the existing score rather than requiring a wholesale re-derivation of the table.

This worked example is limited to three assets. Extending it to the remaining categories in Table 2 and Table 3 is left for

future research once operational access data become available, consistent with the limitation acknowledged in Section 3.4.

7.4 Policy recommendations

In alignment with IKN's formal designation as a strategic national area, several measures require immediate attention. Because Control Systems within the Control Center received the highest composite risk score in this study's assessment, namely 51/70 in Table 3, the highest-priority element of the proposed security standard should be a mandatory redundant command pathway and a segmented or logically isolated network architecture for this specific asset, rather than a uniform standard applied equally across all asset classes. IKN requires a comprehensive special security standard that covers physical, cyber, and hybrid threats, accompanied by a National Mitigation and Contingency Plan that sets out threat-anticipation procedures, unified emergency response chains, clear command lines, and escalation mechanisms for incidents that endanger the continuity of government. These instruments should be grounded in a cross-agency audit of IKN's critical asset inventory, providing the empirical basis for a formal CARVER+Shock assessment [27, 38].

Once core infrastructure becomes operational, the main task shifts from basic preparedness to system-level integration. This includes developing an IC3 based on C4ISR principles and linking it to all critical infrastructure and public service systems, while simultaneously tightening the cybersecurity and data-protection regime that regulates information flows among military, civilian, and commercial actors in IKN. Because the Transmission Subsystem, specifically Towers and Cable Networks, ranked second in this study's risk assessment at 50.5/70 in Table 3, the IC3 rollout during this period should prioritize the integration of transmission-network monitoring sensors before extending coverage to lower-ranked asset categories. Regular joint training and simulation exercises involving TNI, POLRI, BIN, OIKN, and digital infrastructure operators are needed to ensure that these institutional arrangements function as intended [39, 40].

Over the longer term, the aim should be to build a self-sustaining smart defense ecosystem rather than a set of ad hoc projects. Because the CARVER+Shock assessment in Section 6.2 and Section 6.3 consistently ranks Control Systems, the IKN Data Center, and transmission infrastructure as the highest-risk asset categories, long-term investment should prioritize sovereign engineering capacity for control-system and data-center hardware and software before extending the same domestic-development goal to lower-ranked asset categories. This objective requires sustained investment in domestically developed defense technologies to reduce strategic dependence on foreign systems, together with predictable human-resource pipelines connecting defense universities, technical institutes, and national defense agencies. Priority should be given to training specialists in the control-system and data-center domains identified above. In parallel, collaborative research with universities should be used to advance next-generation smart defense methodologies, while international cooperation frameworks should provide channels for sharing good practice, interoperability standards, and smart city security benchmarks with other large urban development programs around the world [26, 38].

Table 4. Illustrative disaggregation of the accessibility parameter for the three highest-ranked assets

Asset	Physical Accessibility	Cyber Accessibility	Supply-Chain Accessibility	Weights (P / C / S)	Weighted Composite
Control Systems (Control Center)	4	7	6	0.3 / 0.5 / 0.2	~6 (Table 3: 6)
Towers and Cable Networks (Transmission)	9.5	6	7	0.6 / 0.2 / 0.2	~8.4 (Table 3: 8.5)
Facilities and Personnel (Control Center)	7	4	7.5	0.5 / 0.2 / 0.3	~6.55 (Table 3: 6.5)

Source: Author's assessment, disaggregating the Accessibility parameter as proposed in Section 7.3.
Note: Component scores and weights are illustrative expert judgments. Weighted composites are rounded and are intended to approximate, not necessarily exactly equal, the corresponding Accessibility entries in Table 3.

8. CONCLUSION

This study has proposed and elaborated an integrated smart defense planning framework for IKN that combines C4ISR architecture with the CARVER+Shock vulnerability assessment methodology. The framework addresses the integration gap identified in the literature review: prior contributions have treated C4ISR and CARVER+Shock as separate analytical tools, leaving their combined application to greenfield urban defense planning insufficiently explored.

The study demonstrates that integrating C4ISR with CARVER+Shock is both analytically coherent and practically necessary for a city such as IKN. The framework is designed to be operationally applicable under real-world constraints, including incomplete data, evolving regulations, and ongoing construction dynamics, enabling practical use by planners in complex and time-sensitive environments. The methodological contribution, namely demonstrating how CARVER+Shock can be adapted to an urban infrastructure context without losing analytical coherence, may prove to be the study's most durable contribution. It opens a pathway for researchers and practitioners who have hesitated to apply a military-origin tool outside its established contexts. The greenfield finding carries a different form of significance. Based on IKN's specific conditions, it suggests that the sequence of security planning matters as much as its content. Building security architecture into a city from the first phase is not merely preferable; it is structurally different from retrofitting, and this difference is likely to influence long-term resilience outcomes.

The vulnerability scores in Table 2 and Table 3, while illustrative, yield a consistent finding: the Control Center and its associated systems represent IKN's highest-priority protection target, followed by data centers and communications transmission infrastructure. These findings should inform immediate decisions on protective investment sequencing, redundancy design, and institutional governance arrangements.

Future research should pursue quantitative CARVER+Shock scoring using empirical data once classified asset information becomes accessible, develop hybrid attack simulation models for IKN, and conduct comparative studies against other smart city security frameworks globally. When IKN's defense systems become fully operational, this framework should be tested not merely as a validation exercise, but as a live stress test against conditions that the current study could only estimate.

ACKNOWLEDGMENTS

The author gratefully acknowledges the opportunities for substantive engagement provided by the Coordinating Ministry for Political, Legal, and Security Affairs of the Republic of Indonesia and the Research and Development Division of BIN, whose discussions informed the practical dimensions of this research.

STATEMENT ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

The author acknowledges the use of AI-assisted language and editorial tools to support drafting refinement and English-language improvement. All analytical judgments, vulnerability assessments, framework propositions, and policy recommendations presented in this study are solely the author's own. The author takes full responsibility for the accuracy, integrity, and scholarly content of the manuscript.

REFERENCES

[1] Syaban, A.S.N., Appiah-Opoku, S. (2023). Building Indonesia's new capital city: An in-depth analysis of prospects and challenges from the current capital city of Jakarta to Kalimantan. Urban, Planning and Transport Research, 11(1): 2276415. https://doi.org/10.1080/21650020.2023.2276415

[2] ANTARA News. (2023). Nusantara smart city blueprint is reference for development: OIKN. https://en.antaranews.com/news/301932/nusantara-smart-city-blueprint-is-reference-for-development-oikn.

[3] ANTARA News. (2025). Gov't committed to develop Nusantara as cyber-secure city. https://en.antaranews.com/news/389401/govt-committed-to-develop-nusantara-as-cyber-secure-city.

[4] Solace Global. (2026). Critical Infrastructure: Rising Cyber and Physical Sabotage Risks. https://www.solaceglobal.com/report/critical-infrastructure-sabotage-risks/.

[5] Soare, S.R., Burton, J. (2020). Smart cities, cyber warfare and social disorder. In Cyber Threats and NATO 2030: Horizon Scanning and Analysis, pp. 108-124. https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.pdf.

[6] Fowler, M.C., Alberts, D.S., Garstka, J.J., Stein, F.P. (1999). Network centric warfare: Developing and leveraging information superiority. Naval War College Review, 53(2): 14. https://digital-commons.usnwc.edu/nwc-review/vol53/iss2/14.

[7] U.S. Food and Drug Administration. (2009). CARVER+Shock Primer: An Overview of the CARVER Plus Shock Method for Food Sector Vulnerability Assessments. https://www.fda.gov/food/food-defense-initiatives/carver-shock-primer.

[8] Azar, E., Moon, C.I. (1984). Third world national security: Toward a new conceptual framework. International Interactions, 11(2): 103-135. https://doi.org/10.1080/03050628408434631

[9] Priyanto, P., Akbar, M., Timur, F.G.C. (2024). Threat perception in Indonesia: Time series analysis of defense doctrines between 1991-2023. Journal of Governance, 9(4): 726-747. https://doi.org/10.31506/jog.v9i4.29873

[10] Hameiri, S., Jones, L. (2013). The politics and governance of non-traditional security. International Studies Quarterly, 57(3): 462-473. https://doi.org/10.1111/isqu.12014

[11] Prasetyo, H., Suharto, P., Santoso, T.I., Al-Mujaddid, S. (2025). Hybrid warfare and total defense strategy: Indonesia's comprehensive security framework in the Indo-Pacific era. International Journal of Humanities Education and Social Sciences, 5(1): 311-321. https://doi.org/10.55227/ijhess.v5i1.1786

[12] Sianturi, K., Saputro, G.E. (2026). Transformation of the Indonesian national army's doctrine and strategy in facing multidimensional threats: Towards the vision of golden Indonesia 2045. Journal of Humanities and Social Studies, 9(1): 138-145.

[13] Batty, M., Axhausen, K.W., Giannotti, F., et al. (2012). Smart cities of the future. The European Physical Journal Special Topics, 214(1): 481-518. https://doi.org/10.1140/epjst/e2012-01703-3

[14] Ou, F., Zhu, X., Li, Q., Yan, R. (2025). Risk assessment of underground utility tunnel projects in Q City using the analytic hierarchy process. Journal of Engineering Management and Systems Engineering, 4(4): 284-303. https://doi.org/10.56578/jemse040405

[15] Maharramov, R., Talibov, A., Hashimov, E. (2025). Application of C4ISR systems in military and security operations. In VII International Scientific Conference Proceeding, pp. 125-134. https://doi.org/10.62731/mcnd-15.08.2025.004

[16] Sowell, P.K. (2000). The C4ISR architecture framework: History, status, and plans for evolution. https://www.mitre.org/sites/default/files/pdf/sowell_evolution.pdf.

[17] Ahmad, H., Dharmadasa, I., Ullah, F., Babar, M.A. (2023). A review on C3I systems' security: Vulnerabilities, attacks, and countermeasures. ACM Computing Surveys, 55(9): 1-38. https://doi.org/10.1145/3558001

[18] Stouffer, K., Pease, M., Tang, C., et al. (2023). Guide to operational technology (OT) security. NIST Special Publication NIST SP 800-82r3. https://doi.org/10.6028/NIST.SP.800-82r3

[19] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. (2015). Guide to industrial control systems (ICS) security. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-82r2

[20] Wysokińska-Senkus, A., Górna, J., Kaźmierczak, M., Mielcarek, P., Senkus, P. (2022). CARVER+Shock and business process management in improving food safety of primary production. Agriculture, 12(7): 1018. https://doi.org/10.3390/agriculture12071018

[21] Mathieu, T.N., Rao, A.S. (2011). Identifying drinking

water and water treatment systems vulnerabilities using the CARVER matrix method. International Journal of Critical Infrastructures, 7(1): 37-49. https://doi.org/10.1504/IJCIS.2011.038955
[22] Inter-American Development Bank. (2016). International Case Studies of Smart Cities: Singapore, Republic of Singapore. https://doi.org/10.18235/0000409
[23] Weinstein, Z. (2017). Digi-Tel—Bespoke technology for connected city of Tel-Aviv. In Citizen Empowerment and Innovation in the Data-Rich City, pp. 159-176. https://doi.org/10.1007/978-3-319-47904-0_10
[24] Inter-American Development Bank. (2016). International Case Studies of Smart Cities: Tel Aviv, Israel. https://doi.org/10.18235/0000416
[25] Das, D., Kwek, B. (2024). AI and data-driven urbanism: The Singapore experience. Digital Geography and Society, 7: 100104. https://doi.org/10.1016/j.diggeo.2024.100104
[26] Shiddiqy, M.A.A., Novarizal, R., Hassan, M.S.N.B.A., Kurniawansyah, D., Alficandra. (2025). An integrated smart defense architecture for the Nusantara Capital City of Indonesia. International Journal of Safety and Security Engineering, 15(12): 2561-2572. https://doi.org/10.18280/ijsse.151213
[27] Pradnyana, H. (2024). A smart defense strategy for Indonesia's new capital amid Asia-Pacific geopolitical tensions. Modern Diplomacy. https://moderndiplomacy.eu/2024/10/01/a-smart-defense-strategy-for-indonesias-new-capital-amid-asia-pacific-geopolitical-tensions/.
[28] Trump, B.D., Poinsatte-Jones, K., Elran, M., et al. (2017). Social resilience and critical infrastructure systems. In Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, pp. 289-299. https://doi.org/10.1007/978-94-024-1123-2_9
[29] Putra, H., Winarna, A., Bonifasius, B., Albrecht, M., Ghazalie, G. (2024). Smart defense 5.0 to strengthen the defense of Indonesia's capital city (IKN). Jurnal Pendidikan: Teori, Penelitian, dan Pengembangan, 9(2): 110-115. https://doi.org/10.17977/jptpp.v9i2.25390
[30] Kitchin, R., Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of Urban Technology, 26(2): 47-65. https://doi.org/10.1080/10630732.2017.1408002
[31] Demertzi, V., Demertzis, S., Demertzis, K. (2023). An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences, 13(2): 790. https://doi.org/10.3390/app13020790
[32] Sensuse, D.I., Putro, P.A.W., Rachmawati, R., Sunindyo, W.D. (2022). Initial cybersecurity framework in the new capital city of Indonesia: Factors, objectives, and technology. Information, 13(12): 580. https://doi.org/10.3390/info13120580
[33] The Jakarta Post. (2024). BRIN explores smart defense concept, AI utilization for IKN. https://www.thejakartapost.com/indonesia/2024/03/07/brin-explores-smart-defense-concept-ai-utilization-for-ikn.html.
[34] Kutoyo, Hanita, M., Daryanto, E. (2025). Strengthening the national air defense system to counter drone threats and air attacks in Jakarta as Indonesia's center of gravity. Multidisciplinary Output Research for Actual and International Issue, 5(4): 6067-6078. https://doi.org/10.54443/morfai.v5i4.4242
[35] International Electrotechnical Commission (IEC). (2009). IEC Technical Specification 62443-1-1:2009: Industrial communication networks—Network and system security—Part 1-1: Terminology, concepts and models. https://webstore.iec.ch/en/publication/7029.
[36] European Parliament and Council of the European Union. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
[37] 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
[38] Nusantara. (2026). U.S. Government Grants US$2.49 Million to Strengthen Nusantara Smart City Planning. https://ikn.go.id/en/posts/us-government-grants-us249-million-to-strengthen-nusantara-smart-city-planning.
[39] Chaudhuri, A., Bozkus Kahyaoglu, S. (2023). Cybersecurity assurance in smart cities: A risk management perspective. EDPACS, 67(4): 1-22. https://doi.org/10.1080/07366981.2023.2165293
[40] Aji, R.P., Supriyadi, A.A. (2026). Integration of defense policy and public policy from a national security perspective in countering hybrid warfare threats. Indonesian Interdisciplinary Journal of Sharia Economics, 9(1): 760-777.

APPENDIX

A. CARVER+Shock scoring calibration framework

A.1 Operational definitions for each parameter level

To make the scoring in Table 2 and Table 3 more transparent and replicable, each CARVER+Shock parameter is calibrated against the five-point interpretive anchors below, consistent with the single-analyst, literature-triangulated procedure described in Section 3.4.

Criticality (C). 1 = disruption has negligible effect on IKN operations; 3 = disruption affects a single sector or district; 5 = disruption produces city-wide cascading failure across multiple critical functions.

Accessibility (A). Following the disaggregation proposed in Section 7.3, this parameter is calibrated separately for physical, cyber, and supply-chain vectors, then combined into a weighted composite. 1 = access requires overcoming hardened, multilayered controls across all three vectors; 5 = at least one vector is effectively unprotected.

Recuperability (R). 1 = full restoration is achievable within hours using redundant systems; 5 = restoration requires months and depends on external resources not currently available to IKN.

Vulnerability (V). 1 = no known technical or procedural exposure; 5 = documented exposure, such as unpatched legacy protocols, absence of redundancy, or unresolved single points of failure, consistent with the smart city physical-security literature referenced in Section 3.3.

Effect (E). 1 = downstream consequences are confined to the asset itself; 5 = downstream consequences propagate across at least two other critical-asset categories identified in Section 4.3.

Recognizability (Rec). 1 = asset function and location are not publicly identifiable; 5 = asset is a publicly documented and easily identifiable target, such as an asset named in the OIKN Smart City Blueprint.

Shock. 1 = an incident would attract limited public or institutional attention; 5 = an incident would generate significant national psychological, economic, and institutional disruption.

A.2 Literature-to-score traceability template

Table A1 illustrates how individual scores in Table 2 and Table 3 can be traced to the literature clusters already identified in Section 3.3. It now covers all seven CARVER+Shock parameters for the three highest-ranked assets in Table 3, namely Control Systems and Towers and Cable Networks, and Table 2, namely the IKN Data Center. These assets account for the top-priority protection targets identified in Section 6.2 and Section 6.3. Extending this traceability exercise to the remaining, lower-ranked assets is left as a direction for future work, since the practical audit value is greatest for the assets that this study identifies as priorities. The reference numbers below are drawn from the 41-study base that informed each asset-level score, allowing readers to audit the scoring rationale directly.

A.3 Cross-parameter consistency notes

Two internal-consistency checks are recommended before final submission. First, assets with higher Criticality should not show disproportionately low Effect scores, since both parameters draw on the same cascading-failure literature cluster. Second, where two distinct assets share an identical sub-score on one parameter, as Control Systems and Towers and Cable Networks both do for Vulnerability at 7.5, as shown in Section 6.3, the accompanying narrative should explicitly identify the parameter or parameters that differentiate their overall ranking.

Table A1. Traceability template linking asset-level CARVER+Shock scores to supporting literature clusters

Asset	Parameter	Score	Literature Cluster	References to Complete
Control Systems	Criticality	9.5	Cascading infrastructure failure	Trump et al.; Kitchin and Dodge; Wysokinska-Senkus et al.; Mathieu and Rao; Shiddiqy et al.
Control Systems	Vulnerability	7.5	Smart-city physical/cyber security	Soare and Burton; Demertzi et al.; Kitchin and Dodge; Ahmad et al.; Chaudhuri and Kahyaoglu
Towers and Cable Networks	Vulnerability	7.5	Smart-city physical/cyber security	Kitchin and Dodge; Demertzi et al.; Maple et al.; Chaudhuri and Kahyaoglu
IKN Data Center	Effect	Very High (5)	Cascading infrastructure failure	Maple et al.; Trump et al.; Sensuse et al.; Inter-American Development Bank (Tel Aviv, Singapore); Shiddiqy et al.
Control Systems	Effect	10	Cascading infrastructure failure	Trump et al.; Maple et al.; Shiddiqy et al.
Control Systems	Shock	7.5	Social resilience & critical infrastructure	Trump et al.; Sensuse et al.
Towers and Cable Networks	Criticality	8.5	Cascading infrastructure failure	Kitchin and Dodge; Trump et al.; Maple et al.
IKN Data Center	Vulnerability	Very High (5)	Smart-city physical/cyber security	Soare and Burton; Demertzi et al.; Ahmad et al.
IKN Data Center	Shock	High (4)	Social resilience & critical infrastructure	Trump et al.; Sensuse et al.; Inter-American Development Bank
Facilities and Personnel (Control Center)	Effect	8.5	Cascading infrastructure failure	Trump et al.; Sensuse et al.; Shiddiqy et al.