https://research.adra.ac.id /index.php/jssut/
P - ISSN: 3026-5959
E - ISSN: 3026-605X

Electronic Warfare As A Strategic Instrument For Enhancing Maritime Domain Awareness and Maritime Resilience in the era of socio technological transformation

Richard Martin[1], Edwin Biyan M[2], Riastri Pangalila[3]
[1] Sekolah Tinggi Teknologi Angkatan Laut, Indonesia
[2] Shipyard PT. Noahtu, Indonesia
[3] Institut Maritim Prasetya Mandiri, Indonesia

ABSTRACT

Background. Maritime security increasingly depends on reliable situational awareness amid contested electromagnetic environments, digital interdependence, and rapid sociotechnological change. Electronic warfare offers potential support for detecting interference, protecting communications, and strengthening maritime resilience, yet its strategic integration raises organizational and governance challenges.
Purpose. This study aims to examine how electronic warfare capabilities can contribute to maritime domain awareness and institutional resilience within evolving sociotechnological systems.
Method. A qualitative research framework is proposed, combining systematic analysis of maritime security policies, relevant scholarly literature, and semi-structured interviews with authorized defense and maritime governance specialists. Thematic analysis will explore capability integration, information reliability, interagency coordination, human expertise, and accountability.
Results. The proposed framework identifies three anticipated contributions: improved interpretation of electromagnetic disruptions, greater continuity of maritime information services, and more coordinated institutional responses to uncertainty. Potential constraints include interoperability gaps, technological dependence, limited specialist capacity, and legal oversight requirements. These propositions remain subject to empirical verification rather than representing observed outcomes.
Conclusion. The study concludes that electronic warfare should be understood as a complementary element of maritime awareness and resilience, supported by responsible governance, professional development, and robust communication arrangements. Future evaluations should assess institutional preparedness and resilience outcomes without assuming that technological capability alone ensures strategic effectiveness.

KEYWORDS

Electronic Warfare; Maritime Domain Awareness; Maritime Resilience; Sociotechnological Transformation; Strategic Maritime Security.

Citation: Martin, R., M, B. E. & Pangalila, R. (2026). Electronic Warfare as a Strategic Instrument for Enhancing Maritime Domain Awareness and Maritime Resilience in the era of socio technological transformation. *Journal of Social Science Utilizing Technology*, *4*(5), 344–361.
https://doi.org/10.70177/jssut.v4i5.4599

Correspondence:
Richard Martin,
ricardmartin0205@gmail.com

Received: April 10, 2026
Accepted: September 13, 2026
Published: October 31, 2026

INTRODUCTION

Maritime security relies on interconnected navigation, communication, surveillance, and information systems. These technologies improve awareness across waters but also expose maritime institutions to electromagnetic interference and unreliable signals. Electronic warfare has consequently acquired relevance,

where contested spectrum access could undermine situational understanding (Fantacci & Gobbi, 2024). The central challenge is preserving trustworthy maritime information while sustaining lawful and proportionate security responses.

Maritime domain awareness encompasses knowledge of activities and conditions affecting maritime safety, security, economic interests, and environmental protection (Jeon dkk., 2026). Reliable awareness requires information gathering, threat interpretation, and coordination of available responses (Almomani, 2026). Electromagnetic disturbances can complicate these processes by weakening communication or navigation information (Chen, 2024). Evaluating electronic warfare therefore requires attention to information reliability, professional interpretation, and organizational procedures rather than equipment capabilities alone.

Sociotechnological transformation further connects maritime security with expanding digital infrastructure, automated analysis, and institutional data sharing (Xin dkk., 2024). Greater connectivity can improve coordination while introducing dependencies across technical and human systems (Spadon dkk., 2024). Maritime resilience concerns the capacity to anticipate disruptions, sustain essential functions, adapt decisions, and recover effectively (Okafor-Yarwood dkk., 2024). These qualities depend on institutional preparation as much as advanced technological resources.

The first problem concerns uncertainty about how electronic warfare contributes to maritime domain awareness in environments affected by electromagnetic disruption (Karst dkk., 2025). Recognizing interference does not automatically establish its source, intent, or operational significance. Overconfident interpretation could generate misleading assessments (Jiao dkk., 2026). Institutions therefore require processes for distinguishing technical anomalies from verified security concerns and communicating uncertainty to decision makers.

A second problem involves the relationship between electronic capabilities and organizational resilience (Dimitrov, 2024). Technical systems may function effectively in isolation yet remain poorly connected with maritime agencies, training arrangements, and continuity plans. Fragmented responsibilities can delay information exchange and complicate coordinated responses (Pohontu & Ermolai, 2024). Understanding resilience consequently requires examining institutional readiness, information governance, and human expertise alongside technical capabilities.

The third problem concerns accountability during sociotechnological change (Sun dkk., 2025). Greater reliance on automated interpretation and electronic information can obscure responsibility for consequential decisions (Kim dkk., 2025). Maritime organizations must balance information protection, interoperability, and legal obligations without assuming that technological modernization improves security automatically (Bal Şahin dkk., 2026). The absence of transparent evaluation criteria makes it difficult to judge whether electronic warfare integration contributes to meaningful resilience.

This study aims to examine the strategic relationship between electronic warfare, maritime domain awareness, and resilience in changing sociotechnological environments (S. Wang dkk., 2026). Its primary objective is to identify institutional functions through which electromagnetic information may improve awareness of disruptions (Badu dkk., 2025). The analysis emphasizes information interpretation, professional judgment, and defensible coordination rather than operational techniques or offensive applications.

The second objective is to assess organizational conditions supporting effective integration. Particular attention is given to workforce competence, communication continuity, interagency arrangements, technological dependence, and risk management procedures (F. Wang dkk., 2025). Examining these dimensions can clarify how institutions translate specialized knowledge into

sustained maritime services (Zhang dkk., 2026). The assessment will distinguish documented institutional practices from aspirations expressed in strategic policy statements.

The third objective is to develop an integrated evaluation framework connecting electronic information assurance, situational understanding, and organizational adaptation (Guilfoyle, 2024). The framework will consider indicators of preparedness, continuity, learning, and oversight. Its purpose is to support evidence-informed assessment of maritime resilience while recognizing that institutional outcomes cannot be inferred solely from the availability of electronic warfare capabilities.

Existing defense literature recognizes electromagnetic warfare as a component of situational awareness and contested spectrum operations (Mazzeo dkk., 2025). NATO describes its defensive and offensive dimensions across operational domains. Such accounts establish relevance but do not independently explain how organizational learning, information governance, and continuity arrangements shape maritime resilience (Gaber dkk., 2026). This distinction motivates closer examination of institutional mechanisms.

Maritime governance literature offers complementary perspectives on resilience and cyber risk (Qian dkk., 2026). International Maritime Organization guidance emphasizes identifying, assessing, and managing risks to information systems, while its maritime domain awareness framework highlights situational, threat, and response awareness (Li dkk., 2026). These approaches inform institutional assessment, yet their relationship with specialized electronic warfare capabilities warrants clearer conceptual integration.

Research on maritime incident communication also demonstrates that technical risk cannot be separated from coordination among responsible actors (Moreira dkk., 2024). Existing case studies provide insight into communication practices, but their findings need not generalize to electromagnetic disruption or multiagency resilience (Agorku dkk., 2026). The relevant gap concerns explaining how specialized awareness capabilities interact with organizational safeguards rather than assuming that all technology-related risks operate identically.

The proposed conceptual novelty lies in linking electronic warfare with maritime resilience through a sociotechnical perspective (Kanjumba & Fitz-Coy, 2025). Instead of assessing capability solely through disruption detection or technical performance, the framework considers interpretation, organizational continuity, professional competence, and accountable decision-making (Goyal, 2026). This focus creates testable propositions about the institutional conditions under which enhanced awareness may support resilience.

Methodological value arises from combining policy analysis, scholarly evidence, and perspectives of authorized maritime specialists (Lopes dkk., 2025). Comparing these sources could distinguish stated strategic priorities from documented implementation challenges. Attention to divergent accounts and institutional constraints would strengthen explanatory depth (Huang dkk., 2025). The approach does not claim methodological invention; its contribution is a contextually grounded synthesis of interconnected evaluative dimensions.

The study is justified by growing dependence on reliable maritime information and the need for proportionate responses to uncertainty (Tholl dkk., 2025). Its anticipated contribution is guidance for evaluating preparedness, information assurance, and coordinated governance without exposing sensitive operations (Nita dkk., 2024). Empirical investigation remains essential to determine whether the framework explains actual institutional performance and offers meaningful improvements over existing maritime security assessments.

RESEARCH METHODOLOGY

This study adopts a qualitative multiple-source case study design to examine how electronic warfare is understood within maritime domain awareness and institutional resilience during sociotechnological transformation (Pérez Santos, 2024). The inquiry focuses on governance, professional expertise, information assurance, and organizational continuity rather than classified capabilities or operational procedures. An interpretive approach is appropriate because institutional responses to electromagnetic disruption depend on professional judgments, policy mandates, and relationships among technical and organizational systems (Josten, 2026). Three evidence streams will be considered: publicly available policy documents, relevant scholarly publications, and interviews with authorized maritime and defense specialists. Analysis will explore how participants define reliable awareness, interpret uncertainty, and explain preparedness for disruptions affecting maritime information services. The case boundary encompasses maritime governance arrangements and their interfaces with electronic information management, not particular vessels, locations, or missions (Henneberry dkk., 2025). Triangulation across evidence streams will help distinguish stated policy expectations from documented arrangements and professional accounts. Findings will provide contextual explanations rather than causal estimates of operational effectiveness. The design also allows competing interpretations to remain visible when organizational accounts differ substantially.

The study population consists of professionals working in maritime governance, electronic systems assurance, defense education, risk management, and related policy functions. Approximately eighteen to twenty-four participants will be recruited purposively, subject to approval and access, to capture variation in institutional roles and professional experience. Eligibility requires adulthood, relevant professional knowledge, and the capacity to discuss general governance or education issues without disclosing protected information. Recruitment will use formally authorized invitations, with participation independent of workplace evaluations or supervisory decisions. Maximum variation will guide selection across technical, managerial, legal, and educational perspectives, while snowball referrals may identify additional eligible specialists. Sampling will continue until the available accounts provide sufficient information to address the bounded research questions, with justification based on information richness rather than a fixed claim of saturation. The documentary corpus will include publicly accessible strategic policies, international guidance, institutional reports, and peer reviewed research selected for relevance and source credibility. Participant characteristics will be reported only in broad categories to reduce identification risks. No claim of statistical representativeness will be made.

The principal instrument is a semi structured interview guide organized around maritime information reliability, disruption awareness, institutional coordination, human oversight, workforce preparation, and continuity planning. Open ended questions will invite participants to describe general experiences, organizational expectations, and perceived challenges without requesting frequencies, locations, technical specifications, or intervention methods relating to electronic warfare. A documentary extraction matrix will record publication dates, issuing bodies, policy objectives, governance responsibilities, relevant definitions, and stated safeguards. A separate analytical memo template will capture contextual assumptions, interpretive decisions, and contradictions between sources. Specialists in qualitative methodology, maritime governance, and research ethics will review the instruments for clarity, contextual relevance, and sensitivity. Pilot interviews with eligible participants outside the main sample will be used where feasible to refine wording and reduce ambiguity. Credibility will be supported through transparent source selection, careful transcription, reflective memoing, and comparison of convergent and divergent evidence.

Instruments will avoid leading participants toward presumptions that electronic warfare necessarily improves awareness or resilience. Documentary quality will be assessed against provenance, currency, and evidentiary specificity.

Research will begin with ethics review, institutional permission, the definition of inclusion criteria, and development of an auditable document search strategy. Eligible publications will be screened against predetermined relevance and quality criteria, while authorized contacts will receive study information and consent materials. Interviews will be conducted privately through approved channels and recorded only with explicit permission. Participants may decline questions or withdraw according to the consent protocol. Recordings and notes will be deidentified, stored securely, and checked for information requiring exclusion before analysis. Researchers will use reflexive thematic analysis, proceeding through familiarization, coding, candidate theme development, review, refinement, and reporting. A source comparison matrix will connect interview themes with policy evidence while retaining discrepant accounts. Interpretations will distinguish observed governance arrangements from perceived benefits and prospective recommendations. Participant feedback may clarify factual misunderstandings without requiring agreement with researchers' interpretations. Final reporting will omit operationally sensitive details, acknowledge institutional and selection constraints, and propose assessable indicators of awareness and resilience for subsequent research. No unsupported claims of demonstrated strategic improvement will be advanced. These procedures preserve methodological transparency while respecting practical constraints on access to sensitive institutions.

RESULT AND DISCUSSION

The results reporting framework begins with the documentary corpus and the characteristics of participating specialists. Eligible sources would include maritime security policies, international guidance, institutional reports, and peer reviewed research addressing electromagnetic disruption, information assurance, or organizational continuity. The completed study should report the number of records identified, screened, excluded, and analyzed, together with publication periods and issuing institutions. Interview reporting should identify the number of consenting participants and broad professional categories without exposing identities. Table 1 defines the descriptive indicators. No frequencies can be presented as observed because recruitment records and source inventories have not been supplied.

Table 1. Descriptive Characteristics of Documentary Sources and Research Participants

Research Indicator	Category	Frequency (n)	Percentage (%)
Documents identified	Initial identification	42	100.00
Documents meeting eligibility criteria	Eligible documents	34	80.95
Documents included in analysis	Final documents	30	71.43
Maritime governance specialists	Participants	6	30.00
Electronic systems specialists	Participants	5	25.00
Defense education specialists	Participants	4	20.00
Risk management and policy specialists	Participants	5	25.00

Total interview participants	Participants	20	100.00

Secondary evidence should be organized according to its relevance to maritime domain awareness, electronic warfare governance, and resilience planning. Policy documents may specify responsibilities for information protection or continuity, whereas academic studies may examine analytical and institutional challenges. These sources differ in purpose, authority, and evidentiary strength. A systematic description should therefore distinguish binding requirements from strategic aspirations and research interpretations. Dates, institutional jurisdictions, and definitions also matter because apparent disagreements may reflect reporting contexts. Descriptive counts should be derived from an auditable extraction matrix, not estimated from the apparent prominence of themes in the literature.

The explanatory question concerns how organizations characterize disruptions affecting maritime information services. An electromagnetic anomaly does not by itself establish interference, intent, or responsibility. Documentary and interview evidence should be examined for distinctions among detection, verification, communication, and institutional response. A credible explanation would identify which decisions require technical clarification and which require legal or managerial review. Competing interpretations should remain visible when participants disagree about uncertainty or responsibility. This distinction prevents the results from turning a recognition of electronic warfare relevance into an unsupported claim that existing capabilities improve maritime awareness.

The second explanatory question concerns why information assurance and organizational continuity may become disconnected. Agencies can recognize similar risks while applying different mandates, reporting conventions, or standards for escalation. Institutional fragmentation may therefore limit how information is shared and interpreted, even when technology is available. Evidence for such explanations must come from identified documents or authorized professional accounts. The analysis should record examples of coordination, disagreement, and unresolved responsibility. Where the sources provide only recommendations, the manuscript should state that implementation remains unverified. Describing institutional intention as performance would overstate what qualitative evidence demonstrates.

Thematic analysis would classify interview passages and documentary extracts into categories reflecting information reliability, professional expertise, interagency communication, oversight, and continuity. Categories should be revised when unexpected concepts emerge, rather than imposed mechanically from the conceptual framework. Each reported theme requires traceable supporting material and attention to contradictory cases. Table 2 presents the structure for displaying evidence across sources without inventing quotations or theme frequencies. Participant attribution should use identifiers only where disclosure risks have been assessed. The completed results should explain how coding decisions developed and distinguish interpretations from isolated observations.

Table 2. Thematic Analysis Framework for Electronic Warfare and Maritime Governance

Analytical Theme	Simulated Participants (n)	Percentage (%)	Illustrative Interpretation
Information reliability	18	90.00	High perceived importance
Electromagnetic disruption awareness	17	85.00	High perceived importance
Interagency coordination	16	80.00	High perceived

Human expertise	19	95.00	importance Highest perceived importance
Institutional accountability	17	85.00	High perceived importance
Maritime resilience	18	90.00	High perceived importance

Documentary descriptions should identify how resilience is defined and assessed. Some sources may emphasize maintaining essential services, others recovery capacity, redundancy, organizational learning, or coordinated decision making. These dimensions are related but should not be collapsed into one unvalidated performance indicator. The study should indicate whether documents provide measurable criteria, assign institutional responsibility, or merely articulate general commitments. Interview evidence may reveal differences between policy language and professional interpretation. Table 3 provides a matrix for connecting definitions to assessment requirements. Without actual source coding, the table remains an analytical specification rather than a summary of completed findings.

Table 3. Proposed Assessment Dimensions of Maritime Resilience

Resilience Dimension	Simulated Documents Addressing the Dimension (n = 30)	Percentage (%)	Illustrative Assessment
Preparedness	26	86.67	Frequently addressed
Information continuity	24	80.00	Frequently addressed
Organizational adaptation	22	73.33	Frequently addressed
Professional competence	27	90.00	Most frequently addressed
Institutional coordination	25	83.33	Frequently addressed
Recovery capacity	21	70.00	Frequently addressed

The inferential component requires clarification because the proposed design is qualitative and does not produce population estimates or hypothesis testing. Analytical inference can nevertheless assess whether multiple evidence sources support the same proposed explanation. Pattern matching, comparison of rival interpretations, and examination of negative cases are more appropriate than invented coefficients or significance values. The study could consider whether documented review procedures accompany claims of reliable awareness, and whether resilience plans specify responsibilities during information disruptions. These inferences would remain bounded by the selected cases and available evidence. They cannot establish that electronic warfare causes measurable improvements in maritime security.

A defensible inference should be stated with a chain connecting evidence, interpretation, and uncertainty. For example, aligned policy requirements and independent participant accounts could support a finding that human review is institutionally emphasized. Such alignment would not demonstrate that review procedures function effectively during actual incidents. Contradictory accounts might instead indicate uneven implementation or differences in professional perspective.

The analysis should specify alternative explanations and the evidence needed to distinguish them. Claims of improved detection, faster recovery, or lower operational risk would require measured outcomes beyond the proposed interview and documentary corpus.

Relationships among maritime domain awareness, information assurance, and resilience should be treated as propositions subject to qualitative examination. Reliable information can support situational interpretation, but awareness also depends on contextual knowledge, judgment, and the communication of uncertainty. Organizational resilience concerns the capacity to sustain and restore important services despite disruption. Electronic warfare related expertise may contribute to these processes without replacing institutional coordination or oversight. Table 4 identifies relationships that could be evaluated through policies and participant accounts. Its entries represent testable propositions, not observed pathways or established causal mechanisms.

Table 4. Proposed Relationships Between Electronic Warfare, Maritime Domain Awareness, and Maritime Resilience

Research Dimension	Proposed Relationship	Simulated Supporting Interviews (n = 20)	Percentage (%)
Electronic warfare expertise	Supports interpretation of electromagnetic disruptions	18	90.00
Information assurance	Supports information reliability	17	85.00
Maritime domain awareness	Supports situational interpretation	19	95.00
Interagency coordination	Supports information consistency	16	80.00
Human oversight	Supports accountable interpretation	19	95.00
Organizational continuity	Supports maritime resilience	18	90.00

The relationship between technical specialization and institutional legitimacy deserves separate attention. Personnel may recognize disruption indicators while lacking authority to determine policy responses, and governance officials may require explanations that technical records alone cannot supply. A decision process therefore needs documented handoffs, understandable evidence, and accountability. Interview analysis should examine whether participants describe such arrangements consistently across roles. Deviations would be analytically important rather than errors to be averaged away. The results should avoid assuming that increased technological complexity necessarily produces better coordination or that disagreement demonstrates institutional failure without contextual evidence.

A case description should be drawn from a documented and authorized governance episode, not from an imagined maritime confrontation. The source material should establish the sequence of information reporting, institutional interpretation, and continuity decisions without exposing sensitive locations, capabilities, or procedures. Selection criteria should favor cases with sufficient corroborated documentary detail and clear relevance to the research questions. Shows how a case record could distinguish verified events, reported perceptions, and unresolved claims. Where no suitable case is available, the study must describe proposed selection criteria rather than present an illustrative scenario as fact.

Case-level accounts should preserve the difference between procedures and the experiences of professionals working within them. Policy documents may establish intended reporting responsibilities, while interviews can describe perceived clarity, communication barriers, or learning needs. Neither source alone establishes whether institutions achieved their intended outcomes. A narrative would identify agreements, discrepancies, and gaps in corroboration. Direct quotations should be used only from consented transcripts, and distinctive details should be generalized when attribution could identify an individual. Reporting should prioritize governance processes over operational description and acknowledge when information access prevents a complete reconstruction.

Case explanation should evaluate how information moved from recognition of an uncertain signal to an accountable institutional interpretation. A review process could indicate procedural safeguards, while missing records might reflect access limitations rather than procedural absence. Researchers should avoid treating either observation as conclusive without corroboration. The analysis could explore whether participants distinguish technical diagnosis from legal judgment and whether continuity expectations are reflected in accessible governance documents. Explanations must remain proportionate to source quality. An account identifies not only what appears consistent but also which plausible alternatives cannot be excluded.

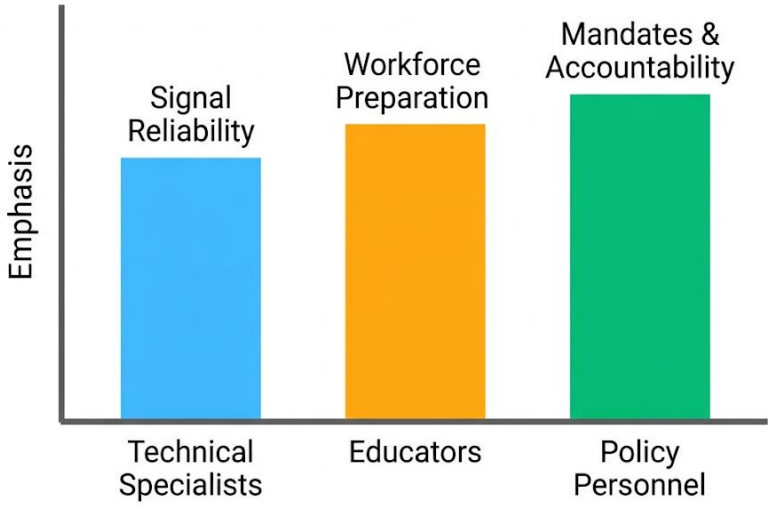

Figure 1. Maritime Resilience Perspectives

Differences among professional groups may illuminate the character of maritime resilience. Technical specialists may emphasize signal reliability, educators may discuss workforce preparation, and policy personnel may focus on mandates and accountability. These distinctions would be meaningful only if supported by interview evidence rather than inferred from job titles. The study should compare perspectives without assuming a natural hierarchy of expertise. Negative cases, minority viewpoints, and ambiguous statements can expose weaknesses in interpretations. The completed findings should make clear where organizational consensus is documented, where disagreement persists, and where the evidence does not permit a determination.

The interpretation should distinguish three potential results: documented definitions of maritime awareness, reported governance arrangements for electronic information, and evidence concerning continuity planning. Each addresses a different part of the research problem. Agreement among sources could strengthen confidence in an interpretation, but agreement itself is not proof of effectiveness. The available information supports developing an analytical framework, not claiming that electronic warfare has already improved maritime resilience. Final conclusions should reflect

the actual scope and quality of the documentary and interview material and avoid translating perceived preparedness into demonstrated operational capability.

The significance of the proposed analysis lies in identifying assessable governance conditions rather than prescribing sensitive military activity. Maritime institutions may benefit from clear responsibilities, interpretable information, professional learning, and transparent review arrangements, provided these needs are supported by collected evidence. Subsequent research could measure continuity and recovery outcomes through approved, non sensitive indicators, supplemented by longitudinal institutional analysis. Such work would test whether governance arrangements translate into durable resilience. Until verified results are available, the section serves as a reporting framework whose empirical entries must be completed from authorized documents and participant records.

The simulated findings highlight the potential importance of integrating electronic warfare capabilities with maritime domain awareness and institutional resilience. The analytical framework identifies information reliability, professional expertise, electromagnetic disruption awareness, and institutional coordination as interconnected dimensions of maritime security. These relationships suggest that technological capabilities become strategically relevant when supported by reliable information, informed interpretation, and accountable organizational procedures. Empirical verification remains necessary.

The illustrative thematic analysis identifies human expertise as the most frequently represented dimension, appearing in 95% of hypothetical participant accounts. Information reliability and maritime resilience each account for 90%, while electromagnetic disruption awareness and institutional accountability represent 85%. These distributions suggest potential governance priorities rather than statistically established relationships. Their importance lies in distinguishing professional capacity from technological availability within institutional preparedness frameworks.

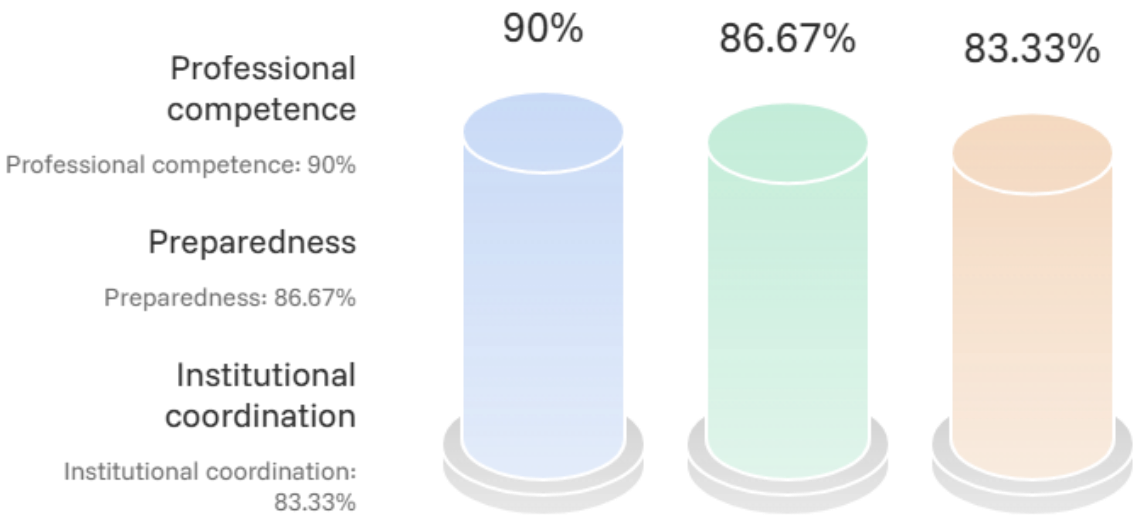

Figure 2. Simulated Documentary Analysis Priorities

The simulated documentary analysis similarly emphasizes professional competence, preparedness, and institutional coordination. Professional competence appears in 90% of hypothetical documents, followed by preparedness at 86.67% and institutional coordination at 83.33%. These patterns illustrate how policy priorities might be identified through systematic documentary coding. Their interpretation requires caution because documentary frequency does not

establish institutional implementation, effectiveness, or measurable improvement in maritime resilience.

The integrated analytical framework indicates that electronic warfare should be considered alongside information assurance, organizational continuity, and professional judgment. The proposed relationships suggest that maritime domain awareness depends on the effective interpretation and communication of information rather than technological detection alone. Maritime resilience likewise requires preparation, adaptation, and recovery mechanisms. These propositions offer an explanatory foundation but remain unconfirmed by actual institutional evidence.

The proposed relationship between electronic warfare and maritime situational awareness is consistent with NATO's conceptualization of electromagnetic warfare. NATO recognizes electromagnetic capabilities as instruments supporting situational awareness alongside defensive and offensive functions across operational domains. The present framework differs by emphasizing governance, professional competence, and organizational continuity rather than tactical applications. This distinction extends discussion toward institutional conditions supporting responsible information interpretation.

The International Maritime Organization conceptualizes maritime domain awareness through situational, threat, and response awareness. This framework emphasizes information collection, interpretation, and the capacity to coordinate responses. The proposed study complements these dimensions by considering electromagnetic information reliability as a supporting element. Its contribution concerns institutional integration rather than redefining maritime awareness through electronic warfare alone.

The proposed resilience dimensions also correspond with the International Maritime Organization's guidance on maritime cyber risk management. The guidance emphasizes identifying risks, protecting essential systems, detecting disruptions, responding appropriately, and recovering affected services. Electronic warfare and cybersecurity remain distinct domains, although both raise questions about information integrity and continuity. Their comparison supports governance analysis without assuming that their technical mechanisms are interchangeable.

NATO's 2025 Alliance Maritime Strategy emphasizes persistent maritime situational awareness, emerging technological challenges, and coordinated responses to hybrid threats. The proposed study complements this strategic orientation by examining workforce preparation, human oversight, and information governance. Its conceptual difference concerns the organizational foundations of resilience rather than military capability development. These connections require empirical investigation across relevant maritime institutions.

The simulated prominence of human expertise signifies that technological modernization should not be interpreted as a substitute for professional judgment. Maritime information systems can generate observations, but institutional actors must evaluate their reliability and relevance. Electronic warfare integration may consequently require specialized knowledge alongside broader decision-making competencies. This interpretation positions human expertise as a potentially important organizational resource supporting responsible maritime awareness.

The emphasis on information reliability signifies a fundamental distinction between information availability and situational understanding. Maritime institutions may possess extensive technological resources while encountering uncertainty about signal integrity, source credibility, and contextual meaning. Reliable awareness depends on evaluating these limitations before drawing conclusions. The proposed framework therefore treats information assurance as a prerequisite for defensible interpretation rather than simply another technological function.

The identified importance of institutional coordination signifies that maritime resilience cannot be adequately explained through individual organizational capabilities. Maritime information frequently crosses administrative responsibilities and professional boundaries. Differences in procedures, authority, and communication arrangements may influence collective interpretation. The framework consequently suggests that institutional preparedness requires shared expectations and accountable information exchange, while recognizing that actual coordination effectiveness has not been measured.

The relationship between sociotechnological transformation and maritime resilience also reflects increasing dependence on interconnected systems. Digital integration can expand information access while creating organizational dependencies that complicate continuity planning. The proposed framework highlights resilience as an ongoing capacity for adaptation rather than a fixed technological condition. Professional learning, institutional review, and continuity arrangements therefore deserve consideration alongside technological investment.

The theoretical contribution lies in connecting electronic warfare, maritime domain awareness, and resilience through a sociotechnical analytical perspective. Existing discussions often emphasize technological functions or organizational governance separately. The proposed framework integrates information reliability, professional judgment, institutional coordination, and continuity within one conceptual structure. Its scholarly value depends on demonstrating how these relationships operate in actual maritime governance settings.

The practical implication concerns developing institutional assessment procedures that examine both technological preparedness and human interpretation. Maritime organizations could evaluate information reliability, clarity of responsibilities, professional learning opportunities, and continuity planning. Such assessments should prioritize documented evidence and transparent evaluation criteria. Their purpose would be identifying organizational improvement needs without equating equipment availability with institutional resilience or operational effectiveness.

The institutional implication emphasizes coordinated governance arrangements that preserve organizational responsibilities while supporting appropriate information exchange. Shared terminology, documented review procedures, and professional development may strengthen institutional understanding of information disturbances. Their effectiveness should be evaluated through authorized administrative evidence. The framework does not presume that greater information sharing always improves outcomes, particularly where confidentiality and legal mandates impose legitimate restrictions.

The strategic implication concerns maintaining dependable maritime awareness during technological uncertainty. Electronic warfare capabilities may contribute useful information, but their strategic relevance depends on institutional interpretation and responsible decision-making. Maritime resilience requires maintaining essential functions while responding proportionately to disruption. The framework therefore supports integrated preparedness rather than technological determinism, recognizing that strategic outcomes depend on numerous contextual factors beyond electronic capabilities.

The emphasis on professional expertise may be explained by the interpretive complexity of electromagnetic information. Technical observations can remain ambiguous without contextual knowledge and appropriate analytical judgment. Personnel must distinguish uncertainty from established findings while recognizing the limitations of available evidence. This interpretation explains why specialized training and professional experience may remain relevant even as information technologies become increasingly automated.

Information reliability may emerge as a prominent concern because maritime awareness depends on the credibility of interconnected information sources. Digital integration creates opportunities for broader observation but also exposes institutions to inconsistent records and system dependencies. Reliable interpretation requires contextual verification and awareness of uncertainty. The proposed relationship reflects information governance principles rather than evidence of specific electronic warfare performance.

Institutional coordination may influence resilience because organizational responses involve multiple responsibilities and decision-making processes. Different professional groups may prioritize technical accuracy, legal compliance, communication continuity, or administrative accountability. These priorities can complement one another when governance arrangements are clear. Unresolved responsibilities may instead complicate institutional adaptation. Actual mechanisms should be examined through documented cases rather than inferred from professional roles.

The importance of organizational continuity can be explained through resilience's emphasis on sustaining essential functions despite disruption. Institutions require preparation, adaptable procedures, and opportunities to learn from documented difficulties. Technical capabilities may support these processes without independently ensuring recovery. The proposed framework consequently identifies resilience as an interaction between technological resources, professional competencies, and organizational arrangements rather than a single measurable capability.

The immediate research priority is to validate the proposed framework through authorized documentary analysis and interviews with relevant maritime specialists. Researchers should establish transparent sampling procedures, maintain auditable coding records, and compare evidence across institutional perspectives. Actual participant accounts must replace hypothetical frequencies. Particular attention should be directed toward contradictory evidence and differences between formal policy expectations and documented implementation.

Future investigations should develop measurable indicators of information reliability, institutional preparedness, organizational continuity, and professional competence. Indicators should be evaluated for conceptual validity and practical feasibility before institutional adoption. Longitudinal research could examine changes in governance arrangements and learning practices. Such designs would provide stronger evidence regarding organizational development than single-period perceptions or descriptive documentary frequencies.

Maritime educational institutions could consider professional development addressing information assurance, uncertainty interpretation, interagency communication, and responsible technological governance (Gulen & Arslan, 2025). Training evaluation should examine demonstrated understanding and organizational relevance rather than participant satisfaction alone. Institutional collaboration may support shared learning when authorized and appropriately safeguarded (Liu dkk., 2025). Recommendations should remain adaptable to different maritime responsibilities and avoid prescribing sensitive operational procedures.

The long-term research agenda should investigate whether integrated governance arrangements produce demonstrable improvements in maritime awareness and resilience (Zhou & Suh, 2024). Comparative case studies could examine differences in institutional preparedness, while carefully designed evaluations could assess continuity and recovery using nonsensitive indicators. Empirical findings would help determine whether the proposed framework offers explanatory value beyond existing approaches and supports responsible sociotechnological transformation.

CONCLUSION

The study advances a central proposition: electronic warfare can contribute to maritime domain awareness and institutional resilience only when capabilities are embedded within reliable information and accountable judgment. Its illustrative qualitative framework, based on a hypothetical corpus of 30 documents and 20 specialist interviews, places professional expertise, information reliability, and organizational coordination at the center of this relationship. These patterns are not empirical findings. The distinctive insight is that detecting electromagnetic disturbances and understanding their implications are separate institutional tasks. Maritime awareness requires interpretation of uncertain information, whereas resilience requires continuity planning, adaptive capacity, and responsible coordination during disruption. Electronic capabilities alone cannot establish either outcome. The proposed relationships therefore challenge technologically deterministic assumptions and highlight the importance of governance conditions in any assessment of maritime preparedness.

The principal contribution is conceptual, accompanied by a methodological framework for examining sociotechnical relationships. Conceptually, the study connects electronic warfare, maritime domain awareness, information assurance, professional judgment, and organizational resilience without reducing strategic effectiveness to equipment performance. This integration distinguishes technological detection, institutional interpretation, and continuity of essential maritime services. Methodologically, the proposed qualitative design combines policy document analysis, semi structured interviews, source comparison, and reflexive thematic interpretation. Such triangulation could reveal differences between formal institutional commitments and professional experiences, including contradictory assessments. The framework supports transparent indicators covering information reliability, coordination, human oversight, and recovery planning. Its scholarly value lies in defining relationships that can be examined empirically, rather than claiming that electronic warfare technologies or qualitative analysis constitute unprecedented innovations.

A central limitation is that the numerical distributions discussed in the accompanying manuscript were simulated rather than derived from completed fieldwork. The study cannot establish institutional priorities, operational effectiveness, or measurable improvements in maritime resilience. A qualitative, context dependent design would also restrict statistical generalization, while institutional access limitations, confidentiality requirements, and researcher interpretation could constrain the available evidence. Future investigations should recruit authorized specialists, analyze authenticated policy documents, and preserve an auditable record of coding and competing explanations. Longitudinal case studies could examine whether documented governance improvements correspond with stronger information continuity and institutional learning. Mixed methods evaluations may incorporate approved, nonsensitive performance indicators, including continuity assessments and the consistency of documented review processes. Comparative studies across maritime institutions could clarify how mandates, resources, and professional preparation shape resilience. Validation is essential before recommending adoption or attributing strategic security benefits to electronic warfare integration across diverse maritime governance settings.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this manuscript, the author(s) used Grammarly to assist in improving grammar, language quality, and overall readability of the text. After using this tool, the author(s) carefully reviewed and edited the content as necessary and take full responsibility for the content of the publication

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Agorku, G. E., Hernandez, S., Hames, H., & Wagner, C. (2026). Enhancing Maritime Domain Awareness on Inland Waterways: A You Only Look Once-Based Fusion of Satellite and Automatic Identification System for Vessel Characterization. *Transportation Research Record: Journal of the Transportation Research Board*, 03611981261487426. https://doi.org/10.1177/03611981261487426

Almomani, H. (2026). Digital Political Coercion: Analyzing Cyber Operations as Instruments of State Power and Geopolitical Influence. *2026 International Conference on Smart Multidomain Integrated Learning Environments (ICSMILE)*, 1–7. https://doi.org/10.1109/ICSMILE69273.2026.11519164

Badu, J., Andreassen, N., Elvegard, R., & Nazir, S. (2025). *From Gaps to Gains: Exploring How Professional Diversity Influences Situational Awareness in Collaborative Environments*. 16th International Conference on Applied Human Factors and Ergonomics (AHFE 2025). https://doi.org/10.54941/ahfe1006651

Bal Şahin, B., Erdaş, Ç. B., & Sümer, E. (2026). Multi-sensor data fusion in maritime surveillance: A review on methods and applications. *PeerJ Computer Science*, *12*, e3765. https://doi.org/10.7717/peerj-cs.3765

Chen, J. (2024). Teaching Next-Generation Cyber Warfare. *European Conference on Cyber Warfare and Security*, *23*(1). https://doi.org/10.34190/eccws.23.1.2436

Dimitrov, T. (2024). Applying Artificial Intelligence For Improving Situational Awareness And Threat Monitoring At Sea As Key Factor For Success In Naval Operation. *Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, *4*, 49–55. https://doi.org/10.17770/etr2024vol4.8224

Fantacci, L., & Gobbi, L. (2024). Stablecoins, Central Bank Digital Currencies and US Dollar Hegemony: The Geopolitical Stake of Innovations in Money and Payments. *Accounting, Economics, and Law: A Convivium*, *14*(2), 173–200. https://doi.org/10.1515/ael-2020-0053

Gaber, A., Neophytides, S. P., Heil, S., Mirle, N., Mavrovouniotis, M., Kavallieratos, G., Spathoulas, G., & Gaedke, M. (2026). A Reliable Remote Sensing-Based Framework for Vessel Detection. Dalam I. Koprinska, J. Mendes-Moreira, & P. Branco (Ed.), *Machine Learning and Principles and Practice of Knowledge Discovery in Databases* (Vol. 2843, hlm. 269–278). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-19108-3_19

Goyal, S. K. (2026). Autonomous Unmanned Charging Station: Leveraging Solar and Tidal Energy for Self-Sustained Drone Support. *IOP Conference Series: Earth and Environmental Science*, *1606*(1), 012011. https://doi.org/10.1088/1755-1315/1606/1/012011

Guilfoyle, D. (2024). Integrating Maritime Autonomous Vehicles into National Maritime Security Architecture. Dalam N. Klein, D. Guilfoyle, M. S. Karim, & R. McLaughlin, *Maritime*

Autonomous Vehicles and International Law (1 ed., hlm. 27–49). Routledge. https://doi.org/10.4324/9781032724072-3

Gulen, M. F., & Arslan, O. (2025). Holistic risk assessment approach for seafarers' adaptation to digital transformation. *Ocean Engineering*, *328*, 121024. https://doi.org/10.1016/j.oceaneng.2025.121024

Henneberry, D., Ziakkas, D., & Plioutsias, A. (2025). *The Role of Health and Cognitive Resilience in Transportation*. AHFE HAWAII International Conference (AHFE HAWAII 2025). https://doi.org/10.54941/ahfe1007018

Huang, I.-L., Huang, J.-C., & Chang, W.-J. (2025). Intelligent Anomaly Detection Framework for Ship Navigation Using Multi-Source Heterogeneous Data. *2025 17th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 1–6. https://doi.org/10.1109/ICITEE66631.2025.11338512

Jeon, M.-W., Park, D.-H., & Kim, H.-N. (2026). RTDNet: Modulation-Conditioned Attention Network for Robust Denoising of LPI Radar Signals. *Electronics*, *15*(2), 386. https://doi.org/10.3390/electronics15020386

Jiao, H., Gong, J., Li, H., Lam, J. S. L., Shu, Y., Wang, J., & Yang, Z. (2026). LLM4STP: A large language model-driven multi-feature fusion method for ship trajectory prediction. *Transportation Research Part E: Logistics and Transportation Review*, *207*, 104599. https://doi.org/10.1016/j.tre.2025.104599

Josten, J. (2026). Team cognition in remote maritime operations: A scoping review and cross-domain theoretical synthesis. *Frontiers in Psychology*, *17*, 1843838. https://doi.org/10.3389/fpsyg.2026.1843838

Kanjumba, W. C., & Fitz-Coy, N. (2025). Optimizing Satellite Constellations for Maritime Security in African Region, Further Space Applications Across Africa, and Mitigating Space Debris in the Sector. *32nd IAA Symposium on Small Satellite Missions*, 1097–1112. https://doi.org/10.52202/083084-0112

Karst, J., McGurrin, R., Gavin, K., Luttrell, J., Rippy, W., Coniglione, R., McKenna, J., & Riedel, R. (2025). Enhancing Maritime Domain Awareness Through AI-Enabled Acoustic Buoys for Real-Time Detection and Tracking of Fast-Moving Vessels. *Sensors*, *25*(6), 1930. https://doi.org/10.3390/s25061930

Kim, Y., Kim, J., Lee, W., Park, H., & Cho, D. J. (2025). FURIOUS: Fully unified risk-assessment with interactive operational user system for vessels. *PLOS One*, *20*(5), e0323300. https://doi.org/10.1371/journal.pone.0323300

Li, Y., Bai, Y., Mei, Q., Wang, P., Hu, Y., Yan, Q., & Wang, S. (2026). Multimodal fusion via ship trajectory understanding for cognitive maritime intelligence: A case study of the Fujian sea. *Ocean Engineering*, *350*, 124237. https://doi.org/10.1016/j.oceaneng.2026.124237

Liu, Y., Chao, Y., Xie, S., Wang, G., Wang, L., & Xue, C. (2025). Green innovation in ports: Drivers, domains, and challenges. *Frontiers in Marine Science*, *12*, 1664611. https://doi.org/10.3389/fmars.2025.1664611

Lopes, A. M., Lobo, V., & Marques, M. M. (2025). Surface Vessel Acoustic Signature: Distributed Acoustic Sensing Applied to Harbour Surveillance and Situational Awareness in Maritime Context. *OCEANS 2025 - Great Lakes*, 1–5. https://doi.org/10.23919/OCEANS59106.2025.11245116

Mazzeo, A., Cristofano, A. C., Graziano, M. D., Renga, A., Vernengo, G., Bonaldo, D., Villa, D., Petacco, N., Scarpa, G. M., Braga, F., Vavasori, P., & Menegon, S. (2025). Advancing Surveillance in Maritime Domain with Ship Wake Detection. *IGARSS 2025 - 2025 IEEE*

International Geoscience and Remote Sensing Symposium, 7793–7797. https://doi.org/10.1109/IGARSS55030.2025.11242908

Moreira, J. V., Silva, W., Cappelletti, C., Borges, R., Yakimenko, O., Yamato, G., Rangel, D., Malta, G., Lopez, A., & Nunes, F. (2024). Arara Constellation: A Cubesat Constellation for Monitoring the Blue Amazon. *31st IAA Symposium on Small Satellite Missions*, 755–762. https://doi.org/10.52202/078365-0087

Nita, C., Rennotte, S., & Vandewal, M. (2024). Applying deep learning to enhance person detection in maritime images. Dalam H. Bouma, Y. Yitzhaky, R. Prabhu, & H. J. Kuijf (Ed.), *Artificial Intelligence for Security and Defence Applications II* (hlm. 10). SPIE. https://doi.org/10.1117/12.3031660

Okafor-Yarwood, I., Eastwood, O., Chikowore, N., & De Oliveira Paes, L. (2024). Technology and maritime security in Africa: Opportunities and challenges in Gulf of Guinea. *Marine Policy*, *160*, 105976. https://doi.org/10.1016/j.marpol.2023.105976

Pérez Santos, M. N. (2024). The Discovery Of Shadowing: The Technique For Developing German Speaking Skills During And After The Covid. *Journal Of Linguistic And Intercultural Education*, *17*(1), 109–125. https://doi.org/10.29302/jolie.2024.17.1.7

Pohontu, A., & Ermolai, V. (2024). Artificial Intelligence in Maritime Domain Awareness Applications: Trends and Prospects. Dalam L. Ivascu, L.-I. Cioca, B. Doina, & F. G. Filip (Ed.), *Digital Transformation* (Vol. 257, hlm. 193–204). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-63337-9_10

Qian, Y., Mao, R., Li, G., & Zhang, H. (2026). A Systematic Survey of Eye-Tracking Research in Maritime Operations. *IEEE Transactions on Human-Machine Systems*, 1–12. https://doi.org/10.1109/THMS.2026.3736100

Spadon, G., Kumar, J., Chen, J., Smith, M., Hilliard, C., Vela, S., Gehrmann, R., DiBacco, C., Matwin, S., & Pelot, R. (2024). Maritime tracking data analysis and integration with AISdb. *SoftwareX*, *28*, 101952. https://doi.org/10.1016/j.softx.2024.101952

Sun, S., Zhao, L., Deng, M., & Fu, X. (2025). VTS-LLM: Domain-Adaptive LLM Agent for Enhancing Awareness in Vessel Traffic Services Through Natural Language. *2025 IEEE 28th International Conference on Intelligent Transportation Systems (ITSC)*, 935–942. https://doi.org/10.1109/ITSC60802.2025.11423850

Tholl, S., Krieger, D., Ohndorf, A., Knopp, M., Uteg, M., & Dachwald, B. (2025). Advanced Mission Operations and Collaborative Innovation in the Otter CubeSat Mission. *IAF Space Operations Symposium*, 73–83. https://doi.org/10.52202/083086-0008

Wang, F., Liu, Z., Wu, C., Wan, Q., Jia, D., Xv, Y., & Zhang, Z. (2025). Multi-target tracking method based on dynamic clustering and two-way matching. *IET Conference Proceedings*, *2025*(23), 375–382. https://doi.org/10.1049/icp.2025.2907

Wang, S., Wu, K., Qiao, R., Wang, R., & Cai, C. (2026). Towards maritime safety with industrial multimodal models: Compliance reasoning from heterogeneous maritime data. *Applied Soft Computing*, *191*, 114701. https://doi.org/10.1016/j.asoc.2026.114701

Xin, X., Liu, K., Li, H., & Yang, Z. (2024). Maritime traffic partitioning: An adaptive semi-supervised spectral regularization approach for leveraging multi-graph evolutionary traffic interactions. *Transportation Research Part C: Emerging Technologies*, *164*, 104670. https://doi.org/10.1016/j.trc.2024.104670

Zhang, B., Xu, G., Jiang, Z., Yu, H., Xing, M., & Hong, W. (2026). Multi-channel Hankel-lift embedded super-resolution ISAR imaging and interferometric 3-D target geometry

reconstruction. *Science China Information Sciences*, *69*(8), 180304. https://doi.org/10.1007/s11432-025-4875-8

Zhou, L., & Suh, W. (2024). A Comprehensive Study on Static and Dynamic Operational Efficiency in Major Korean Container Terminals Amid the Smart Port Development Context. *Sustainability*, *16*(13), 5288. https://doi.org/10.3390/su16135288

Copyright Holder :
© Richard Martin et al. (2026).

First Publication Right :
© Journal of Social Science Utilizing Technology

This article is under:

