International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

The Psychology of Defensive Cyber Deception Technology Adoption Across IT and OT Environments

Daniel Ward

Department of Computer Science, Southern New Hampshire University, United States

Author Email: d.ward@snhu.edu

Abstract-- Defensive cyber deception is often described as a technical capability, but its adoption depends on how people interpret an intentionally deceptive security practice. This paper reframes cyber deception adoption as a psychological and perceptual problem involving awareness, trust, risk appraisal, perceived control, ethical legitimacy, self-efficacy, and decision confidence. The study combines secondary quantitative analysis of an existing deidentified survey dataset from ICS/OT professionals with an integrative synthesis of cyber deception literature from IT, security operations center, and operational technology contexts. The quantitative analysis found that perception-based factors explained substantially more variance in adoption readiness and effective utilization than education, years of experience, or sector. Self-efficacy and direct experience were the strongest predictors, followed by instructional support, performance expectancy, and security trust. The literature synthesis showed that IT and SOC adoption concerns center on workflow fit, use-case clarity, analyst confidence, and signal trust, while OT adoption concerns center on safety, operational control, and perceived risk. The paper proposes a Defensive Cyber Deception Acceptance Model that positions category awareness, legitimacy appraisal, trust, perceived control, and decision confidence as the psychological pathway through which deception technology becomes acceptable in practice.

Keywords: adoption psychology, cyber deception, decision confidence, operational technology, perceived control, security trust, self-efficacy, technology acceptance

I. INTRODUCTION

Defensive cyber deception is unusual because it asks security professionals to accept a technology that works by placing intentional falsehoods into a defensive environment. A decoy host, honey credential, false engineering file, or simulated service is not valuable solely because of what it technically is. It is valuable because of what it causes human actors to believe, test, avoid, distrust, or investigate. For attackers, deception can distort the perceived environment. For defenders, deception can transform an ambiguous security event into a signal that appears more intentional and actionable.

This makes cyber deception a psychological technology as much as a cybersecurity technology. Its success depends on mental models, trust, perceived legitimacy, perceived control, risk tolerance, and decision confidence. A defender who does not understand what cyber deception is may classify it as an outdated honeypot, a trick, a compliance problem, or an operational hazard. A leader who does not understand how deception improves signal quality may view it as a discretionary tool rather than as a way to reduce uncertainty. A security analyst may value the clarity of a decoy interaction, while an operations engineer may first ask whether the same system can be safely bounded and governed.

The psychology differs by environment. In enterprise IT and security operations centers, the central question is often whether deception improves analyst workflow, reduces alert ambiguity, and fits existing decision processes. In operational technology (OT), the first psychological question is frequently whether the technology can be trusted in a safety-sensitive environment. OT professionals may be less concerned with novelty and more concerned with control: where the deception asset is placed, who owns it, whether it can touch production processes, and whether it will create confusion during operations.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

The purpose of this paper is to develop a psychology-centered view of the adoption of defensive cyber deception across IT and OT environments. The paper does not propose another architecture or control framework. Instead, it examines why professionals may accept, resist, trust, distrust, or misunderstand deception technologies. It uses existing survey data from ICS/OT professionals as the quantitative anchor. It integrates IT, SOC, and OT deception literature to develop a cross-domain model of perception-based adoption.

II. PSYCHOLOGICAL FOUNDATIONS

A. Defensive Cyber Deception as Perception Management

Cyber deception is built around perception management. Ferguson-Walter et al. examined decoy-based and psychological cyber deception with professional red teamers. They found that deception can alter attacker behavior when both decoys and information about deception are present. That finding matters for adoption psychology because it demonstrates that deception is not only a passive sensor. It changes how people reason about the environment and what actions they believe are safe, useful, or risky.

Cranford et al. framed cyber deception as a cognitive problem involving decisions under uncertainty and deceptive signals. This perspective shifts the adoption question. The issue is not merely whether a platform can deploy decoys. The issue is whether defenders believe the deceptive signal will create useful uncertainty for attackers while creating sufficient clarity for defenders.

B. Trust, Risk, and Perceived Control

Trust is central because defensive deception intentionally introduces false artifacts into a security environment. Professionals must believe that those artifacts are authorized, bounded, documented, observable, and reversible. Without that belief, deception may be perceived as a source of uncertainty rather than a tool for reducing uncertainty.

Risk appraisal is also central. A deception asset can be understood as a detection opportunity or as a possible operational burden. The same technical control may be interpreted positively in an enterprise environment and cautiously in OT. This is not irrational resistance. It reflects context-specific risk perception. In OT, the consequences of tool misplacement, ambiguous alerts, or unapproved communication paths can be more serious than in ordinary enterprise networks.

Perceived control connects trust and risk. Professionals are more likely to accept deception when they believe they can define its scope, monitor it, explain it, remove it, and prevent it from interfering with legitimate operations. This suggests that deception adoption is strongly related to control beliefs and self-efficacy rather than solely to security awareness.

C. SOC Decision-Making and Psychological Fit

Reeves and Ashenden studied cyber deception in the context of security operations centers. They found that adoption is limited by a lack of clear use cases, limited empirical evidence, reluctance to embrace active defense, vendor overpromising, and concern about interrupting SOC analyst decision-making. Their work is important because it places deception adoption squarely inside organizational psychology and naturalistic decision-making rather than treating it as a purely technical configuration problem.

From this perspective, a deception alert is a sensemaking object. It helps an analyst decide whether an observed action is accidental, routine, suspicious, or adversarial. A decoy interaction can reduce ambiguity because legitimate users should not interact with the object. The psychological value is not that the alert is technologically exotic; it is that the alert carries a different inference structure.

D. Category Awareness and Ethical Legitimacy

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

Category awareness is a persistent problem. Many professionals still understand defensive deception through narrow mental models such as legacy honeypots, research traps, or attacker lures. The United Kingdom National Cyber Security Centre reported confusion around terminology in its cyber deception trials. It noted that inconsistent vocabulary makes it harder for organizations to understand what they are trying to achieve. This terminology problem is psychological because people cannot trust or adopt a technology category they cannot clearly name.

Ethical legitimacy is another adoption condition. Reid et al. argued that cyber deception technologies influence human cognition and behavior, thereby raising ethical issues, even when used defensively. In adoption terms, professionals must perceive deception as proportionate, authorized, and directed at adversary behavior rather than as an uncontrolled form of manipulation inside the organization.

III. RESEARCH QUESTIONS AND HYPOTHESES

Four research questions guided the paper:

RQ1. Which perception-based factors are associated with adoption readiness and effective utilization of defensive cyber deception technology in the ICS/OT dataset?

RQ2. Do perception-based factors explain adoption readiness and effective utilization beyond demographic and professional characteristics?

RQ3. Which perception-based predictor has the strongest unique relationship with adoption readiness and effective utilization?

RQ4. Which perception themes recur across IT, SOC, and OT cyber deception adoption literature?

The quantitative portion tested three hypotheses:

H1. Performance expectancy, self-efficacy/direct experience, social influence, instructional support, and security trust will each be positively associated with adoption readiness and effective utilization.

H2. Perception-based predictors will significantly improve the prediction of adoption readiness and effective utilization beyond education, years of experience, and sector.

H3. Self-efficacy/direct experience will be the strongest unique predictor in the full model.

IV. MATERIALS AND METHODS

A. Research Design

This study used a secondary quantitative analysis and an integrative literature synthesis. The quantitative component reanalyzed an existing deidentified dissertation dataset collected from ICS/OT professionals. The synthesis component integrated research on cyber deception, SOC decision-making, attacker cognition, ethics, and OT adoption constraints to generalize the psychological model beyond the OT-only dataset.

No new participants were recruited, and no new survey responses, interviews, focus groups, or private operational records were collected. The design is therefore appropriate for a non-new-human-research extension. The quantitative analysis provides empirical evidence about perception-based adoption factors in a specialized OT population, while the literature synthesis provides the cross-domain IT/SOC context.

B. Dataset and Psychological Constructs

The secondary dataset originated from a quantitative dissertation study of deception technology adoption among ICS/OT professionals. The original study used UTAUT to examine perceptions of technology adoption, including usefulness, ease of use, social influence, facilitating conditions, awareness, skill, and adoption/effective utilization.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

The present analysis reinterpreted those variables as psychological adoption constructs. Performance expectancy represented perceived utility. Self-efficacy/direct experience represented confidence derived from experience and skill. Social influence represented perceived normative support. Instructional support represented perceived availability of guidance and learning resources. Security trust represented the belief that deception technology is secure and dependable. The outcome variable was adoption readiness and effective utilization.

Table 1. Psychological interpretation of secondary-analysis constructs

Construct	Psychological interpretation	Role in adoption
Performance expectancy	Utility appraisal: belief that deception improves detection or response.	Increases perceived value of use.
Self-efficacy/direct experience	Confidence in one's ability to understand, operate, or interpret deception.	Reduces uncertainty and increases readiness.
Social influence	Perceived peer, stakeholder, or leadership support.	Creates normative legitimacy.
Instructional support	Availability of guidance, training, playbooks, or learning resources.	Makes adoption feel controllable and teachable.
Security trust	Belief that deception is safe, dependable, and not itself a risk source.	Supports acceptance in high-consequence contexts.

C. Statistical Tests

Pearson and Spearman correlations were used to test bivariate associations between perception-based variables and adoption readiness/effective utilization. Hierarchical ordinary least squares regression tested whether perception-based predictors improved prediction beyond education, years of experience, and sector. HC3 robust standard errors were used for coefficient-level inference in the full model. Complete regression cases totaled N = 262.

The synthesis portion used directed thematic interpretation. Literature was coded for recurring perception themes: awareness, use-case credibility, trust, perceived risk, perceived control, ethical comfort, analyst workflow fit, safety legitimacy, and decision confidence.

V. RESULTS

A. Bivariate Tests

All five perception-based predictors were positively associated with adoption readiness and effective utilization, supporting H1. The strongest bivariate relationship was self-efficacy/direct experience, followed by instructional support and social influence. These results suggest that acceptance of defensive cyber deception is closely tied to perceived capability rather than to technical exposure.

Table 2. Bivariate associations with adoption readiness and effective utilization

Predictor	Pearson r	p	Spearman rho	p
Performance expectancy	.491	< .001	.393	< .001

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

Self-efficacy/direct experience	.699	< .001	.610	< .001
Social influence	.563	< .001	.566	< .001
Instructional support	.567	< .001	.487	< .001
Security trust	.490	< .001	.490	< .001

B. Hierarchical Regression Tests

The hierarchical regression supported H2. Demographics and professional characteristics explained little variance. When perception-based factors were added, the model explained 64.3 percent of the variance in adoption readiness and effective utilization. The increase in explained variance was statistically significant, indicating that adoption readiness was substantially more psychological than demographic in this dataset.

Table 3. Hierarchical regression results

Model/Test	Model specification	Primary statistic	p value	Interpretation
Demographics-only model	Education, experience, sector	R2 = .028; F(5, 256) = 1.46	p = .205	Demographics alone did not significantly explain adoption readiness.
Full psychological model	Demographics plus performance expectancy, self-efficacy/direct experience, social influence, instructional support, security trust	R2 = .643; adjusted R2 = .629	p < .001	The perception-based model explained a substantial proportion of variance.
Model improvement	Full model compared with demographics-only model	Delta R2 = .616; F change(5, 251) = 86.64	p < .001	Perception-based predictors significantly improved prediction.

C. Unique Predictors

H3 was supported. Self-efficacy/direct experience was the strongest unique predictor in the full model. Instructional support, performance expectancy, and security trust were also significant. Social influence was positively associated at the bivariate level but was not statistically significant after stronger predictors were controlled. This pattern suggests that social approval may matter early in adoption, but direct confidence, support, perceived utility, and trust matter more when predicting readiness.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

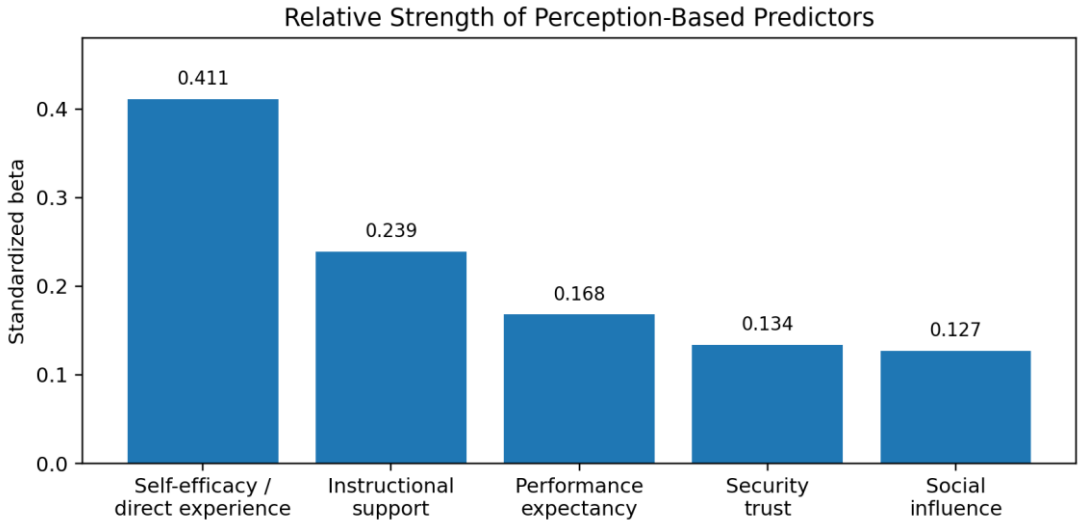

Fig. 1. Standardized predictor strength in the full psychological model

D. Cross-Domain Perception Themes

Table 4. Cross-domain perception themes

Theme	IT / SOC emphasis	OT emphasis	Psychological meaning
Category awareness	Understanding what deception is and how it differs from ordinary monitoring.	Avoiding the assumption that deception equals unsafe honeypots in production.	Professionals need a usable mental model before they can evaluate the technology.
Use-case credibility	Clear analyst workflow and evidence that alerts reduce ambiguity.	Clear operational boundary and evidence that decoys do not affect live process control.	Adoption depends on perceived fit with existing work.
Trust	Trust that deception alerts are high-fidelity and useful for triage.	Trust that deception is safe, bounded, and approved.	Trust is both signal trust and system safety trust.
Perceived control	Ability to tune, route, explain, and measure deception events.	Ability to constrain, document, retire, and govern deception assets.	Control beliefs reduce perceived adoption risk.
Decision confidence	Confidence to escalate or investigate based on deception signals.	Confidence to act without disrupting operations.	Deception is accepted when it improves judgment under uncertainty.

The synthesis showed that IT/SOC and OT environments share the same psychological adoption chain but weigh the chain differently. IT and SOC adoption centers on whether deception improves analyst sensemaking. OT adoption centers on whether deception is safe and controllable. In both cases, the technology must be perceived as legitimate, bounded, and useful before it becomes operationally acceptable.

VI. DEFENSIVE CYBER DECEPTION ACCEPTANCE MODEL

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

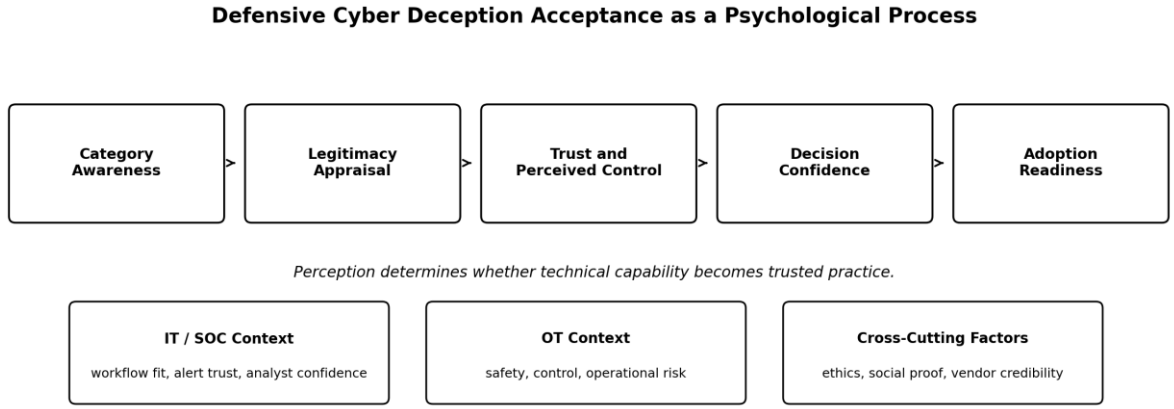

Fig. 2. Defensive Cyber Deception Acceptance Model

The model places category awareness at the beginning of adoption. If professionals do not know what defensive deception is, or if they rely on outdated honeypot stereotypes, later judgments about usefulness, risk, trust, and control become distorted. Legitimacy appraisal follows: professionals must decide whether intentional defensive deception is appropriate, authorized, and ethically defensible.

Trust and perceived control form the central psychological mechanism. Professionals are more likely to accept deception when they trust the signal and believe the technology can be governed, constrained, explained, and removed. Decision confidence is the final psychological bridge between acceptance and use. A deception signal becomes valuable when it helps defenders decide that an event deserves attention, escalation, or investigation.

VII. DISCUSSION

A. Deception Adoption Is a Psychological Problem

The main implication is that defensive cyber deception should not be understood only as a tool category. It is a psychological intervention in a security environment. It changes the attacker's uncertainty, but it also changes the defender's interpretation. That dual effect explains why adoption is difficult: the same system that creates clarity for defenders also intentionally creates false artifacts.

The quantitative findings support this interpretation. General credentials and demographics did not explain adoption readiness nearly as well as self-efficacy, instructional support, perceived utility, and security trust. In practical terms, professionals do not become ready for deception because they hold a degree or have years of general experience. They become ready when they understand the technology, trust it, can practice with it, and believe they can control it.

B. The Awareness Problem

A recurring adoption barrier is that many professionals lack a modern category for defensive deception. If a decision-maker thinks only in terms of old honeypots, then modern decoys, honeytokens, identity lures, cloud lures, and OT-safe canary artifacts may be misunderstood. This produces a perception gap: the technology may be useful, but the category is not yet psychologically legible.

This is why terminology matters. Inconsistent language forces professionals to make adoption decisions without stable mental models. A psychological adoption strategy should therefore begin with category clarification before product selection.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

C. IT and OT Are Different Psychological Contexts

In IT and SOC environments, deception adoption is tied to analyst workflow. Professionals ask whether the tool reduces alert fatigue, creates reliable signals, and improves response confidence. The perceived risk is often workflow disruption or poor signal quality.

In OT environments, adoption is tied to safety and controllability. Professionals ask whether the system can be deployed without affecting uptime, deterministic communication, equipment, operators, or process safety. The perceived risk is not simply false positives; it is the possibility that a security tool may create operational uncertainty in an environment where uncertainty is costly.

D. Implications for Training and Product Communication

The results imply that training should not begin with product features. It should begin with mental models: what deception is, what it is not, why a decoy interaction is meaningful, how false artifacts are governed, and what a defender should do when a deception event occurs. Hands-on labs, alert interpretation exercises, tabletop scenarios, and bounded OT-safe examples are more likely to build self-efficacy than general awareness materials.

Vendors and security leaders should also avoid presenting deception as magic or as a replacement for existing controls. Overpromising can damage trust. A more psychologically effective message is that deception creates a specific kind of signal that can reduce ambiguity when integrated with governance, monitoring, and response processes.

VIII. LIMITATIONS

The quantitative portion used secondary data collected for an ICS/OT dissertation rather than a new cross-domain IT/OT survey. As a result, the statistical findings are strongest for ICS/OT professionals and should not be generalized directly to all SOC or enterprise IT populations. The IT and SOC portions of the paper are based on an integrative literature synthesis rather than on new primary data.

The measures were adapted from an existing technology-adoption survey rather than from a purpose-built cyberpsychology instrument. Future research should directly measure ethical comfort, perceived legitimacy, category awareness, alert trust, ambiguity reduction, and decision confidence. A future IRB-approved study could use vignette experiments to compare ordinary security alerts, deception alerts, and enriched deception alerts across IT, SOC, and OT participants.

IX. CONCLUSION

Defensive cyber deception adoption is not only a technology problem. It is a psychological problem involving how professionals understand, trust, appraise, and act on intentional defensive falsehoods. Across IT, SOC, and OT contexts, deception must become psychologically legible before it becomes operationally accepted.

The secondary analysis showed that perception-based factors, especially self-efficacy/direct experience, instructional support, perceived utility, and security trust, explained adoption readiness far better than demographics alone. The literature synthesis showed that IT/SOC and OT environments share core perception barriers but differ in emphasis. IT and SOC professionals focus on workflow and signal confidence, while OT professionals focus on safety, control, and operational legitimacy.

The Defensive Cyber Deception Acceptance Model offers a psychology-centered way to understand those differences. Deception technologies will be adopted more successfully when organizations build awareness, legitimacy, trust, perceived control, and decision confidence before expecting defenders to operationalize the tools.

X. DECLARATIONS

Funding: No external funding was received for this work.

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 20-28 DOI: https://doi.org/10.63671/ijsssr.v4i2.623
Volume: 4 | Issue: 2
July-September 2026

Conflicts of interest: The author declares no conflicts of interest.

Ethical statement: This article uses a secondary analysis of an existing deidentified dissertation dataset and an integrative synthesis of published literature and public guidance. No new human participants were recruited, and no new human-subject data were collected.

Data availability: The underlying deidentified secondary dataset derives from prior dissertation research and is not included in the manuscript package. Aggregated results are reported in the article.

Generative AI assistance: Generative AI assistance was used to support organization and formatting. The author reviewed, edited, and approved the final manuscript and remains responsible for the accuracy, integrity, originality, and source attribution of the article.

REFERENCES

1. Cranford, E. A., Gonzalez, C., Aggarwal, P., Tambe, M., Cooney, S., & Lebiere, C. (2021). Towards a cognitive theory of cyber deception. Cognitive Science, 45(7), e13013. https://doi.org/10.1111/cogs.13013
2. Ferguson-Walter, K. J., Major, M. M., Johnson, C. K., & Muhleman, D. H. (2021). Examining the efficacy of decoy-based and psychological cyber deception. Proceedings of the 30th USENIX Security Symposium, 1127-1144. https://www.usenix.org/conference/usenixsecurity21/presentation/ferguson-walter
3. National Cyber Security Centre. (2025, December 11). Cyber deception trials: What we have learned so far. https://www.ncsc.gov.uk/blog-post/cyber-deception-trials-what-weve-learned-so-far
4. Reeves, A., & Ashenden, D. (2023). Understanding decision making in security operations centres: Building the case for cyber deception technology. Frontiers in Psychology, 14, 1165705. https://doi.org/10.3389/fpsyg.2023.1165705
5. Reid, I., Okeke-Ramos, A., & Serafin, M. (2024). Exploring the ethics of cyber deception technologies for defensive cyber deception. In Proceedings of the 10th International Conference on Socio-Technical Perspectives in Information Systems, 140-148. https://ceur-ws.org/Vol-3857/
6. Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. MIS Quarterly, 36(1), 157-178. https://doi.org/10.2307/41410412
7. Ward, D. (2025). Enhancing security: A comprehensive study on deception technology integration in manufacturing and critical infrastructure [Doctoral dissertation, University of the Cumberlands]. ProQuest Dissertations & Theses.
8. Ward, D. (2026a). A Deception Readiness Index for ICS and OT cybersecurity programs. International Journal for Research in Applied Science and Engineering Technology, 14(VI), 2401-2406. https://doi.org/10.22214/ijraset.2026.83810
9. Ward, D. (2026b). A workforce readiness model for deception technology in ICS and OT cybersecurity programs. International Research Journal of Engineering and Technology, 13(6), 610-614. https://www.irjet.net/archives/V13/i6/IRJET-V13I0693.pdf
10. Ward, D. (2026c). Deception architecture for water and wastewater operational technology environments. International Journal of Engineering Research and Technology, 15(6). https://doi.org/10.5281/zenodo.20745399
11. Ward, D. (2026d). Operationalizing deception technology in ICS/OT: A control mapping framework for critical infrastructure cybersecurity. International Journal of Soft Computing and Engineering, 16(3), 1-9. https://doi.org/10.35940/ijsce.C3723.16030726