

Enhancing Consciousness of Cybersecurity

Leveraging the Vedic Knowledge Trinity

Sharda S. Nandram · Puneet K. Bindlish
Nyenrode Business Universiteit · Vrije Universiteit Amsterdam

CENTRAL PROPOSITION

Know the context.
Question the unknown.

A proposed framework connects the knower, the knowable and ways of knowing in cybersecurity.



Read the research

01 Background and question

Cybersecurity involves people’s interpretations and actions as well as technical systems. The paper explores how awareness of knowledge and its limits could broaden organisational responses to cyber threats.

RESEARCH QUESTION

How can the Vedic knowledge trinity enrich reflection on cybersecurity behaviour and preparedness?

02 Conceptual framework

The trinity

Knower · knowable · knowledge.

The K-continuum

Known, unknown and limits of knowing.

The proposed framework combines reflective CAARS prompts with four PARC qualities: proactive, adaptive, resilient and connected. The focus is the organisation and its people as potential victims.

03 Evidence and method

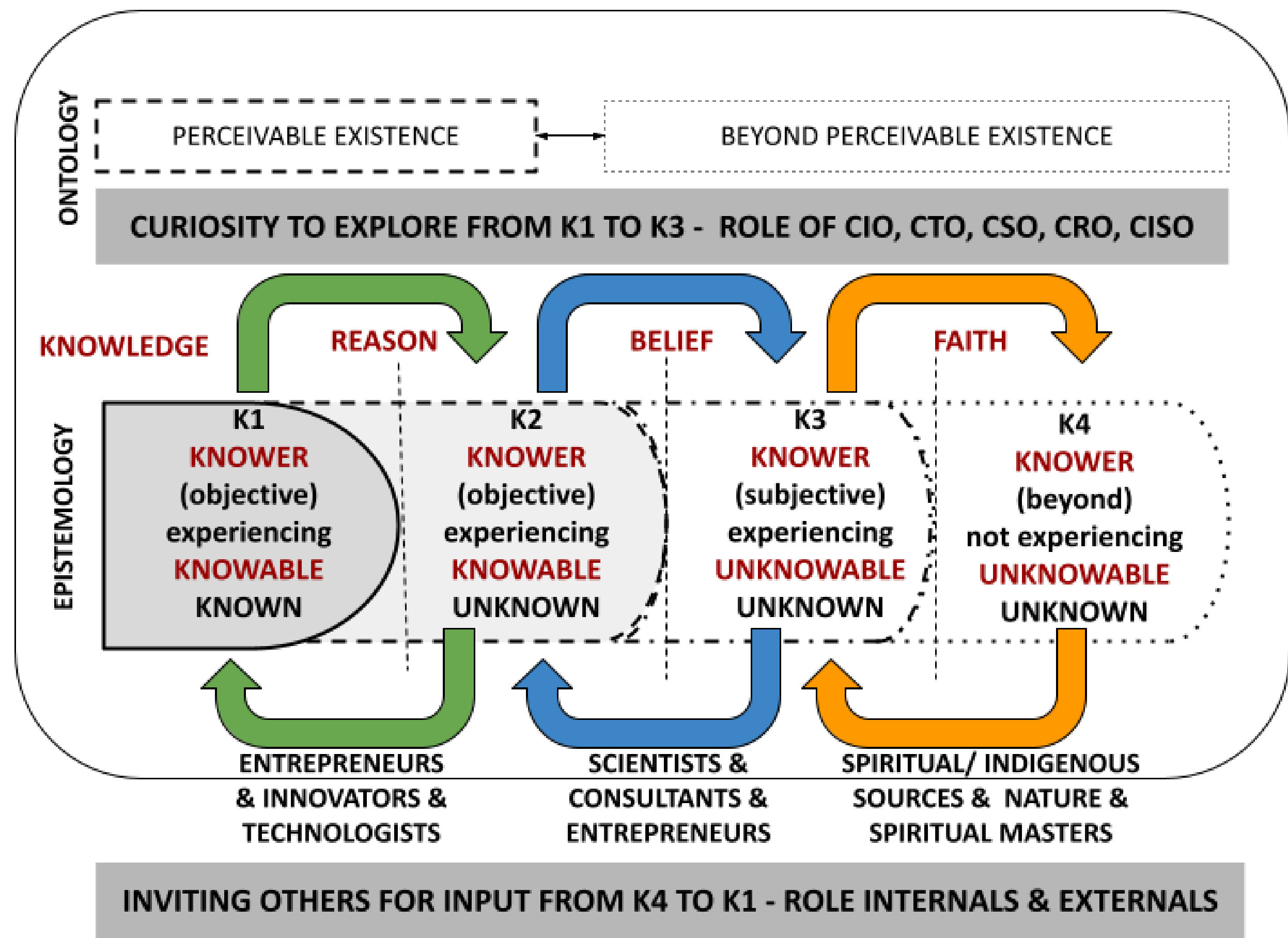
Conceptual design-science work limited to problem identification and framework design, informed by critical realism and interpretation of selected Vedic texts.

The first author’s participation in an MBA class with 15 other management participants informed problem understanding. The proposed framework was not subsequently demonstrated or evaluated in an intervention.

04 The original K-continuum

The authors’ conceptual model connects categories of the unknown with the knower, knowable and knowledge.

Figure 2 K-continuum with knower, knowable, knowledge



Source: Adapted from Nandram (2022)

Original Figure 2, [1], p. 33. The paper adapts this illustration from Nandram (2022), cited as [4].

Proactive	Adaptive	Resilient	Connected
Anticipate.	Respond.	Recover.	Relate.

05 Findings and contributions

A Place the person in context

The trinity brings the observer, the domain of concern and the process of knowing into the same frame.

B Recognise different unknowns

The K-continuum distinguishes what is known, knowable, experienceable and beyond experience.

C Connect reflection with readiness

CAARS and PARC offer a conceptual structure for examining assumptions, actions and preparedness.

06 Discussion

The framework invites security leaders to reflect on context, external drivers, assumptions, actions and sources of knowing. Its philosophical contribution can complement established security practices; improved protection remains a proposition to test.

07 Limitations and next steps

No security-performance improvement is demonstrated. Future research needs operational definitions, practical implementation and evaluation of behavioural and organisational outcomes.

CONCLUSION

The knowledge trinity offers a proposed lens for cybersecurity reflection; its practical effectiveness requires empirical evaluation.

SELECTED REFERENCES

[1] Nandram, S. S., & Bindlish, P. K. (2024). Enhancing consciousness of cybersecurity: leveraging the Vedic knowledge trinity. International Journal of Technology Transfer and Commercialisation, 21(1), 14-39. doi:10.1504/IJTTTC.2024.10066715.

[2] Hevner, A. R., et al. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.
[3] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

[4] Nandram, S. S. (2022). Spirituality: The Discipline for Doing Business with the Unknown. Inaugural lecture, Nyenrode Business Universiteit.