Critical realism in the fabric of cybersecurity

A. Kayode Adesemowo[1][0000-0003-1217-1651]

SOAMS Consulting, South Africa

kadesemowo@soams.co.za

Abstract

Security breaches continue day in and day out unabated as the headlines beam in our faces. The 2022 update to the ISO27002 takes cybersecurity seriously more than ever before. Not only that, ISO27002:2022 acknowledges contextualizing by categorizing into four areas of Organization, Technology, Physical, and People (OTPP). The socio-technical aspects of cybersecurity is brought to the fore. Critical realism has made inroad in information systems; a discipline acknowledged to be socio-technical in nature. The same cannot be said of cybersecurity. This research investigates how critical realism is used in cybersecurity (information security), to what extent it is used, and how it can be leveraged. The review, a hybrid systematic-scoping review, leverage systematic review platforms, Python libraries for pattern and clusters. In emphasizing context over content, the review screening identified nuances: intra citations among authors, intransitivity of digital technology, emergent mechanisms requiring attention in cybersecurity

Keywords: critical realism, explanatory, cyber risk, cybersecurity, information security, context, digital technologies, digital transformation

"***Introducing the Battleground... and the Road to Peace?*** *Since its infancy, IS research has struggled to reconcile the simultaneous technological and social nature of information systems*" – Cecez-Kecmanovic et al., 2014, p. 810

Introduction

Security breaches continue day in and day out unabated as the headlines beam in our faces. They practically occur unabated, as if they might become a 'new normal'. The ISO 27002:2022 has now included cybersecurity in its name while missing definitions (Adesemowo, 2021) for essentials such as information assets, IT assets, and cybersecurity. Hopefully, they will come through in ISO27000, the nominal 'standard' for all ISO2700x suites of standards. What we must not miss, though, is the contextualisation in the ISO 27002: 2022. Cyber or cybersecurity is no longer 'hanging' in the ISO2700x suites. More importantly, ISO 27002:2022 contextualises the cybersecurity (information security) domain: Organisation, Technological, Physical, and People (OTPP). These four broad categorisations 'control' the 93 controls, out of which 11 are new, 24 were merged and 58 controls revised from the previous ISO 27002:2013.

The ISO 27002 contextualisation provides an opportune moment for researchers (and practitioners alike) to consider critical realism, and to engage with evolving dynamic nature of digital technologies (Adesemowo, 2021; Baskerville et al., 2020). More especially, the dialectical intransitivity and transitivity dimensions of critical realism (Bhaskar, 2013; Dobson, 2001). Readers are referred to articles that have explained critical realism in-depth among many writeups (Bhaskar, 2013; Mingers, 2001; Preko & Boateng, 2020; Wynn & Williams, 2020) while noting (Archer et al., 2013; Smith, 2006)Body of the paper

Research domain

Critical realism no longer sits in the peripheral; it has increasingly made its way into the information systems domain with special conference tracks and calls for papers in journals, including the 'basket of eight'. However, there has not been a commensurate investigation into how critical realism is used in- and can advance cybersec/infosec. The research question is:

... *"Is critical realism (CR) used in cybersecurity/information security, or to what extent is CR used, and how can CR leverage infosec/cybersec studies"*...

The research question is against the backdrop that 'non-technical' aspects of cybersecurity are socio-technical in a similar light to information systems (where critical realism has made an inroad)

2.1   Methodology: Hybridized scoping review
The aim is to gain understanding into the 'how' of CR use in cybersec/infosec with an emphasis on governance. It is not so much of the 'what'. For this study, two things of interest in its approach are considering full-text availability as part of the title-abs-key screening and the balancing act of finding a tilting middle ground between systematic and scoping review by leveraging the PRISMA-sCR guideline (Tricco et al., 2018). Nonetheless, the rigor, validity, 'explicity', and reproducibility entrenched in a systematic review were not discarded entirely. This paper was guided by the three phases of 'planning', 'conducting', and 'reporting' (Brereton et al., 2007; van Dinter et al., 2021)

Findings and way forward
The search conducted in March 2022 yielded 124 articles. Upon review according to the protocol, twenty-four papers were included for full-text screening and data extraction. The review process is presented in Fig. 2, and the spread of included papers in Fig. 1. Multi-layered review approach in ReLiS (Bigendako & Syriani, 2018) facilitates rigor and reproducibility, and reduces bias.

In emphasizing context over content, the review screening identified nuances: intra citations among authors, intransitivity of digital technology, emergent mechanisms requiring attention in cybersecurity.
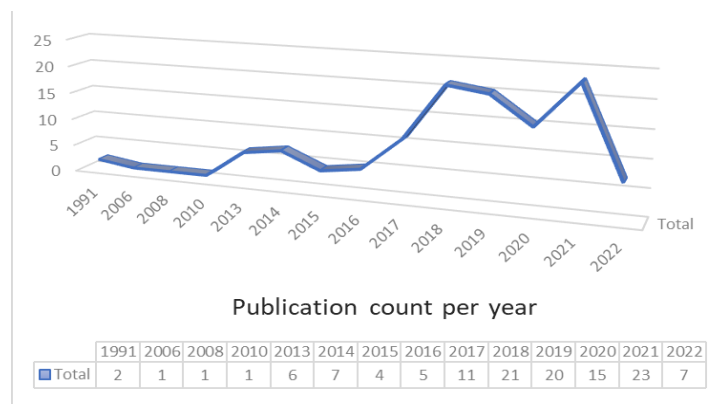

	1991	2006	2008	2010	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Total	2	1	1	1	6	7	4	5	11	21	20	15	23	7

Fig. 1. Screening: n=124 papers count per year, excluding reverse-search (snowballing based on Larsen et al. (Larsen et al., 2019)
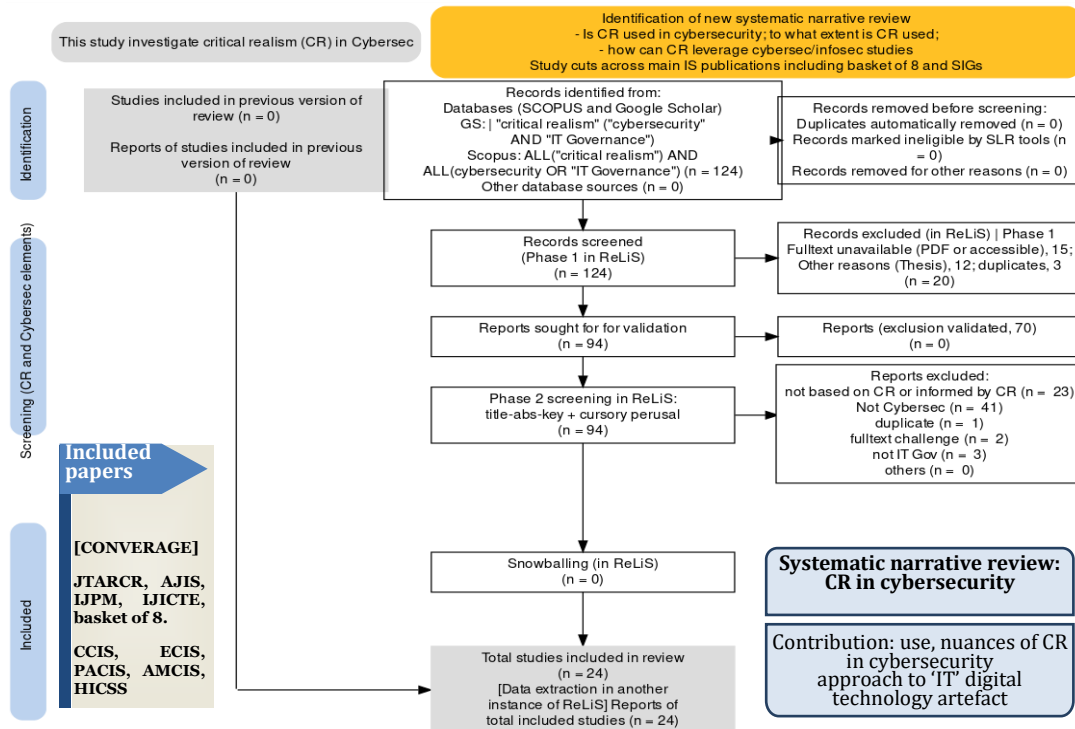
Fig. 2. Modified PRISMA-based flowchart highlighting the review process: [Flowchart drawn with Haddaway's toolkit (Haddaway et al., 2021; Page et al., 2021) and modified manually]

References

Adesemowo, A. K. (2021). Towards a conceptual definition for IT assets through interrogating their nature and epistemic uncertainty. *Computers & Security*, *105*, 102131. https://doi.org/10.1016/j.cose.2020.102131

Archer, M. S., Bhaskar, Roy, Collier, Andrew, Lawson, T., & Norrie, A. (Eds.). (2013). *Critical Realism: Essential Readings* (2nd ed.). Routledge. https://doi.org/10.4324/9781315008592

Baskerville, R., Myers, M. D., & Yoo, Y. (2020). Digital First: The Ontological Reversal and New Challenges for Information Systems Research. *MIS Quarterly*, *44*(2), 509–523. https://doi.org/10.25300/MISQ/2020/14418

Bhaskar, R. (2013). *A Realist Theory of Science* (revised). Routledge. https://books.google.co.za/books?id=7318AgAAQBAJ

Bigendako, B. M., & Syriani, E. (2018). Modeling a Tool for Conducting Systematic Reviews Iteratively. In S. Hammoudi, L. F. Pires, & B. Selić (Eds.), *MODELSWARD 2018: Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development* (pp. 552–559). ScitePress. https://doi.org/10.5220/0006664405520559

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

Dobson, P. J. (2001). The Philosophy of Critical Realism—An Opportunity for Information Systems Research. *Information Systems Frontiers*, *3*(2), 199–210. https://doi.org/10.1023/A:1011495424958

Haddaway, N. R., McGuinness, L. A., & Pritchard, C. C. (2021). *PRISMA2020: R package and ShinyApp for producing PRISMA 2020 compliant flow diagrams.*

https://doi.org/10.5281/ZENODO.5082518

Larsen, K. R., Hovorka, D. S., Dennis, A. R., & West, J. D. (2019). "Understanding the Elephant: The Discourse Approach to Boundary Identification and Corpus Construction for Theory Review Articles." *Journal of the Association for Information Systems*, *20*(7), 887–927. https://doi.org/10.17705/1jais.00556

Mingers, J. (2001). Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research*, *12*(3), 240–259. https://doi.org/10.1287/isre.12.3.240.9709

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *PLOS Medicine*, *18*(3), e1003583. https://doi.org/10.1371/JOURNAL.PMED.1003583

Preko, M., & Boateng, R. (2020). Assessing healthcare digitalisation in Ghana: A critical realist's approach. *Health Policy and Technology*, *9*(2), 255–262. https://doi.org/10.1016/J.HLPT.2020.03.006

Smith, M. L. (2006). Overcoming theory-practice inconsistencies: Critical realism and information systems research. *Information and Organization*, *16*(3), 191–211. https://doi.org/10.1016/J.INFOANDORG.2005.10.003

Tricco, A. C., Lillie, E., Zarin, W., O, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Annals of Internal Medicine*, *169*(7), 467–473. https://doi.org/10.7326/M18-0850

van Dinter, R., Tekinerdogan, B., & Catal, C. (2021). Automation of systematic literature reviews: A systematic literature review. *Information and Software Technology*, *136*, 106589. https://doi.org/10.1016/J.INFSOF.2021.106589

Wynn, D. E. J., & Williams, C. K. (2020). Recent Advances and Opportunities for Improving Critical Realism-Based Case Study Research in IS. *Journal of the Association for Information Systems*, *21*(1), 50–89. https://doi.org/10.17705/1jais.00592