Describing a CyberSA Analysis Model

Dr Cyril Onwubiko
Secretary – IEEE United Kingdom & Ireland
Chair – Cyber Security Intelligence, Research Series Limited

11-June-2018

C-MRiC.ORG®
Centre for Multidisciplinary Research, Innovation and Collaboration

Context

Confusion / Misconception	Direction / Guidance
• Most things are branded CyberSA when they are not. • Mechanisms that underpin evidence collection or gathering are often labelled CyberSA, when, in fact, they are not. E.g. Big data repository, data collection etc. • Mechanisms that enable intelligence sharing are often regarded as CyberSA, when they are not. E.g. Intelligence Sharing Partnerships, Threat Intelligence, and CTI	• CyberSA Definitions / Processes and Examples (See Ref. 3-5) • CyberSA Requirements – FR and NFR (See Ref. 2) • CyberSA Building Blocks & Re-usable Artefacts • CyberSA Standardisation Initiative – IETF / RFC / Large Consortia etc

Requirements

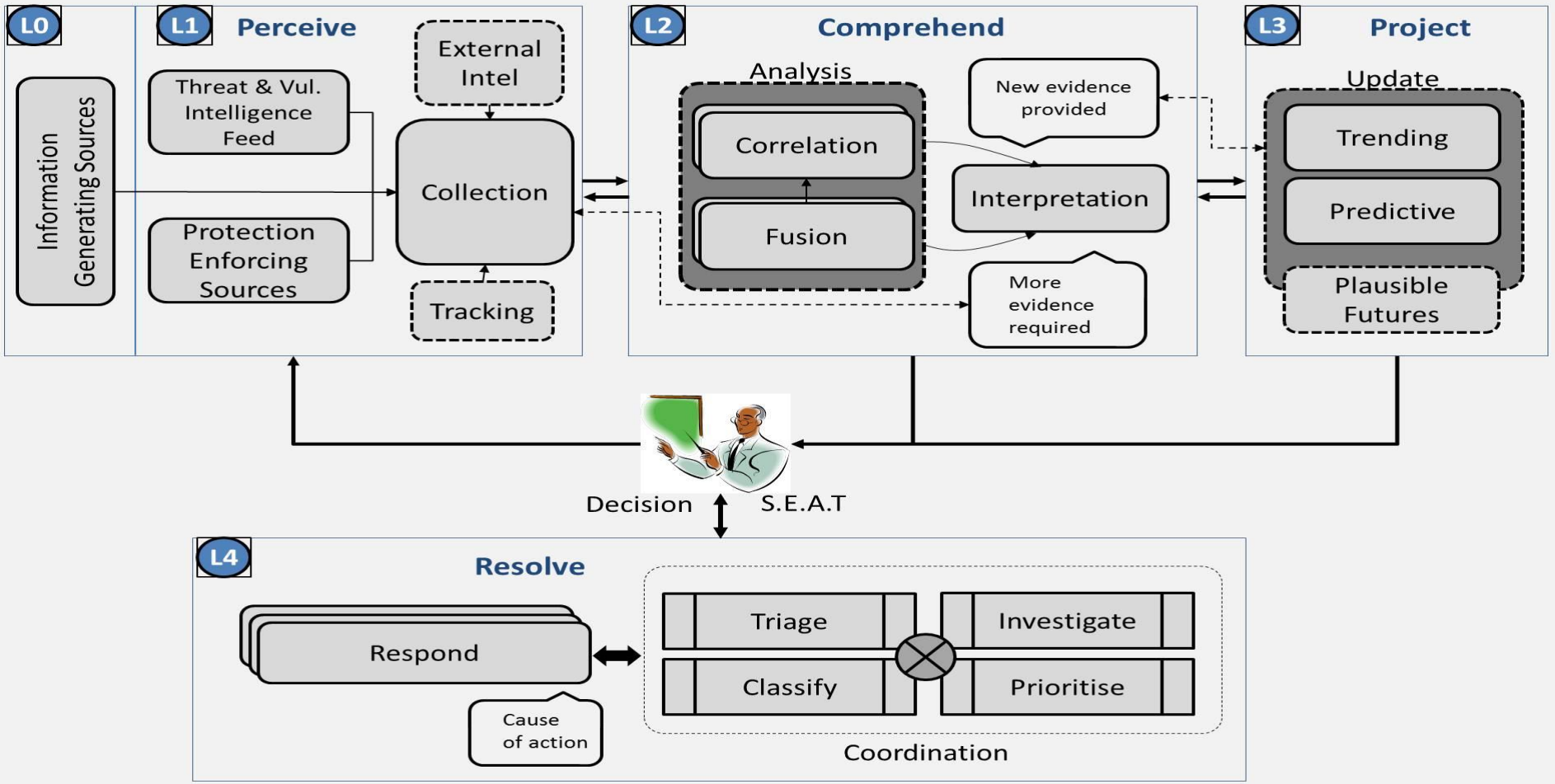
- Consistency
- Quality
- Repeatability
- Reliability
- Interoperability
- Conformity
- Open Process
- Productisation
- Industrialisation

- Relevance
- Foundation
- Fundamental building blocks
- Measurable
- Tools
- Terms
- Metrics
- Robust
- Transparency

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

CyberSA Analysis Model



C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Conclusion

- Cyber Situational Awareness is a multidisciplinary specialism – comprising human factor, cognition, cyber experts, HCI, complexity theorist, data scientists etc.
- Dealing with multi-dimensional problems and issues, complex situations that often require, pace, speed and accuracy.
- We need a standardisation effort aimed at harmonising our collective collaborative efforts to address our current problems.

Thank you!

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

Future Work

Facilitate Standardisation through IEEE Standards Association / Working Groups on Cyber Situational Awareness

C-MRiC.ORG®

Centre for Multidisciplinary Research, Innovation and Collaboration

References

1. Onwubiko, C. (2016). Understanding Cyber Situation Awareness. *International Journal on Cyber Situational Awareness, Vol.1. No. 1, 2016.*
2. Onwubiko, C. (2009). Functional Requirements of Situational Awareness in Computer Network Security. *IEEE International Conference on Intelligence and Security Informatics. ISI '09, Dallas, TX, USA 8-11 June 2009.*
3. Onwubiko, C. and Owens, T. J. (eds). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications.* IGI-Global, 2011.
4. Jajodia S., Liu P., Swarup V., and Wang C. (eds). *Cyber Situational Awareness: Issues and Research (Advances in Information Security)*. Springer 2009
5. Endsley, M. R. and Garland D. J. (eds). *Situation Awareness Analysis and Measurement*. Reprinted 2008 by CRC Press.