Designing for Cyber Situational Awareness: Initial Results of a Literature Review

Mikko Salminen
National Defence University, Helsinki, Finland

mikko.k.salminen@mil.fi

Abstract: Situational awareness is the prerequisite for decision making. According to the widely used theory by Mica Endsley, situational awareness can be segmented to three levels: 1) perception of elements of the environment in time and place, 2) understanding of the meaning of the situation formed by the elements, and 3) evaluation of the development of the situation. Systems for common operational picture (COP) have various functionalities for processing, mediating, analysing, and visualizing data with the goal to enable the decision makers to form situational awareness and understanding. Compared to other domains (e.g., land, air, naval), in the cyber domain the phenomena need novel types of visualizations and a map is not often the most suitable visualization platform. There is paucity of previous studies comparing the amount of research on cyber COP to the other operational domains. In addition, previous studies have not summarized the extant literature on methods to support decision makers' metacognitive processes with cyber COP functionalities and visualizations. To address these gaps, the identified COP functionalities from the existing literature were classified following the 3-level model of situational awareness. In addition, previous studies on supporting the metacognitive processes, such as evaluating information novelty or credibility, by COP functionalities were identified. High research activity was observed for the COP within the cyber domain. In majority of the papers, the COP functionalities for cyber situational awareness were presented on a conceptual level with no evidence on implementation of them or their possible effectiveness in supporting the work of the situational awareness operators or the decision makers. This is a gap that calls for more research. Taken together, these findings can be used in steering future research for developing systems that support cyber situational awareness more effectively.

Keywords: Cyber situational awareness, Situational understanding, Common operational picture, Information visualization, Military decision making

1. Introduction

Decisions are preceded by situational awareness, which can be segmented to three levels: 1) perception of elements in the current situation, 2) comprehension of the situation, and 3) projection of the future state of events (Endsley, 1995). In addition, there are various cognitive processes that may affect the mentioned three levels of situational awareness and the following process of decision making. Various, conscious or unconscious, metacognitive processes may form the evaluation of certainty of own situational awareness and the credibility or recency of the information that it is based on (e.g., Rousseau et al., 2010). There are sets of design guidelines for designing situational awareness systems, which also give suggestions to support these cognitively resource-demanding processes.

Endsley and Jones (2012), for example, offer a list of 50 design guidelines for situation awareness oriented design (SAOD). In this set there are various guidelines to support the processing of the three levels of situational awareness, but also for supporting the metacognitive processes. For example, in the SAOD it is suggested that the user should be supported in evaluating the credibility of different sensors that produce information, that the recency of the presented information should be shown, and missing information should be marked. It is suggested that these mentioned design guidelines support the metacognitive processes of evaluating information qualities, the quality of own situational understanding, and even the questioning of it.

The aim of this study was to examine what is the state of research within the systems supporting cyber situational awareness, and whether there are already findings on effectiveness of certain design choices in supporting different levels of situational awareness and the related metacognitive processes. That is, to see if there is empirical evidence for the design guidelines that are aimed at supporting situational awareness.

1.1 Cyber Situational Awareness and Cyber Common Operational Picture

Compared to more traditional domains of land, air, and naval, the cyber domain is rather new. However, there is already research on cyber-specific situational awareness. Franke and Brynielsson (2014) define cyber situational awareness as a subset of general situational awareness that concerns the cyber environment. They also mention, that the cyber situational awareness may be formed based on information from various sources, from technological sensors as well as from human informants. As with other types of information that support the forming of situational awareness, also with cyber situational awareness the central type of system or medium for mediating and presenting information is the common operating picture (COP). COP can be defined

loosely as a collection of "actively selected information that is useful to multiple stakeholders with a common overarching mission" (Varga et al., 2018). COP can be seen as a storage place for information or more like a process of negotiating meaning of various information for the users (Varga et al., 2018). Often, however, COP is considered to be a certain single display that is shared and that facilitates collaborative planning and operating (e.g., Conti et al., 2013).

1.2 Objective of the Current Study

Cyber COP has been studied previously, for example, by Franke and Brynielsson (2014). However, they didn't relate the findings to other operational domains and they didn't classify the findings following the three-level model of situational awareness. On the other hand, this classification was used in a survey study by Varga et al. (2021) and in a more recent review by Jiang et al. (2022). The unique contribution of the current study is to include comparison to the other operational domains, and also including the supporting of metacognitive processes with the cyber COP functionalities.

Thus, the aim of the current study was to examine the relative extent of literature on cyber situational awareness compared to studies on situational awareness in other domains. Also, within the previous studies on cyber situational awareness the aim was to map how the three levels of situational awareness, as defined by Endsley (1995), are supported by various cyber COP functionalities. In addition to the three levels of situational awareness, also the supporting of metacognitive processes by the cyber COP functionalities was surveyed within the existing literature.

2. Methods

2.1 First Literature Review on COP in Various Domains

The literature review consisted of two stages. In the first stage the extent of literature about the common operating picture was examined following the guidelines of PRISMA procedure (Moher et al., 2010). This initial collection of publications was conducted in 2023. With search terms "common operating picture" or "common operational picture", peer-reviewed papers in journals and conference proceedings were searched from the 10-year period 2013 – 2023, using the following databases: ACM, IEEE, ProQuest, and ScienceDirect.

Only those papers were included which described at a minimum a concept of a COP, or listed knowledge requirements for a COP. Those papers were excluded, which only mentioned the COP without any further description of its functionalities, visualizations, or information types which it should be able to process.

From the included papers, following information was collected:

- Citation
- Type of the publication (journal, conference proceedings)
- Context (army, navy, air force, joint, cyber, information operations, other)
- Level of warfare (battleground technical, tactical, operational, strategic)
- Readiness level (concept or user requirements, a functioning prototype, a prototype which has been shown to be effective, in operative use)
- Visualizations and functionalities by the level of situational awareness that they support

2.2 Second Literature Review on Cyber COP

The second literature review was targeted to previous cyber common operational picture studies. The aim was to map the current status of research in this field, with emphasis on identifying how the functionalities of the cyber COP systems can support the human processing of the three levels of the situational awareness, as defined by Endsley (1995) and also the metacognitive processes. In addition, the aim was to identify the so-called evidence readiness level of the studies on cyber COP, ranging from whether the described systems were presented on merely a conceptual level or whether they were in operational use with demonstrated effects on improving the situational awareness and understanding of the decision makers.

The search was done in January 2025 to the IEEE Publications and the ACM Digital library databases, since these two sources were identified as the most fruitful sources in the initial literature search, described in the preceding section. The literature was searched from the previous 10 years (2015 – 2025) from peer-reviewed journal papers and papers published in conference proceedings. The search term was: "common operational picture" OR "common operating picture" AND cyber. The inclusion criteria were similar with the first literature review, as described above. The following information was collected from the included papers:

- Type of the publication (journal, conference proceedings)
- Level of warfare (battleground technical, tactical, operational, strategic)
- Readiness level (concept or description, a functioning prototype, a prototype which has been shown to be effective, in operative use)
- Levels of situation awareness (1-2-3) that were supported by the described functionalities and visualizations

3. Results

3.1 Initial Literature Review on Various Contexts

The numeric results of the first literature review are presented in Figure 1.

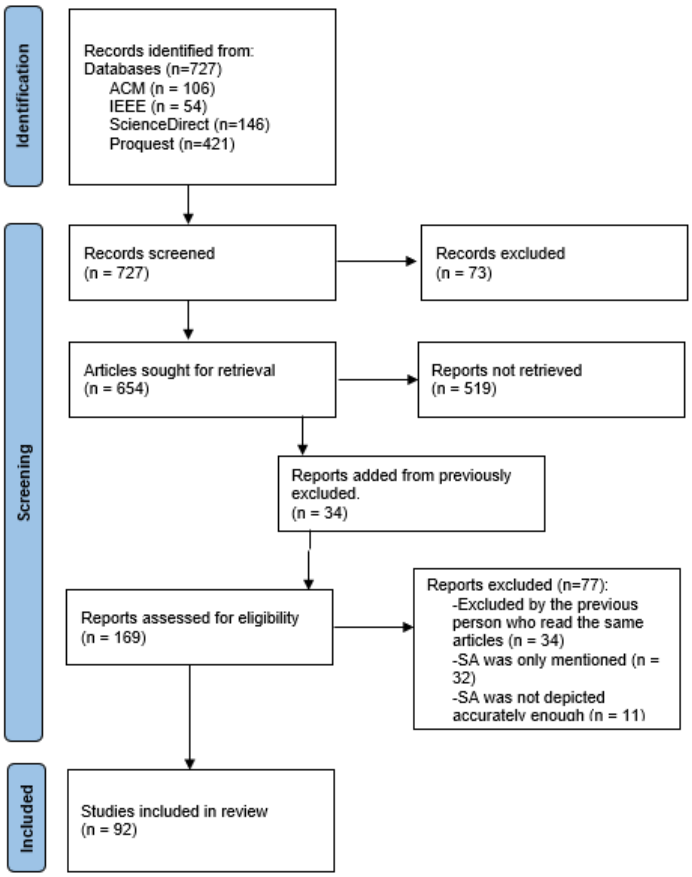

Figure 1: Result of the first literature review

Most of the exclusions were made because the screened paper merely mentioned COP without describing it or its functionalities in such detail that it would have been possible to identify which level of situational awareness was being supported. Since situational awareness is such an essential concept in the military leadership and command & control, it was expected that it would appear in numerous studies.

In Table 1 is presented the numbers of papers for each readiness level of the COP concept or system they described.

Table 1: Number of identified papers for each readiness level of the described COP application

Readiness level	Number of papers
1. Concept, list of user requirements	31
2. Working prototype	25
3. Prototype that has been studied	22
4. In operative use	4
5. In operative use, with proven effectiveness	0

The number of papers decreased linearly for the higher readiness level. That is, majority of papers presented either a concept or a prototype with less studied focusing on actual effectiveness the presented COP system. This could reflect the fact that the COP systems that are implemented in the military domain may have functionalities that are classified and the effectiveness of such systems is reported in internal classified reports.

Table 2 shows the number of papers for each context. Most of the papers reported of a COP system for the purpose of presenting situational information in the army domain, and cyber domain was the second most numerous category.

Table 2: Number of identified papers for each context

Context	Number of papers
Army	37
Navy	8
Air	2
Joint	6
Cyber	19
Info	1
Other	16

In Table 3 are presented number of papers where COP functionalities supporting the different levels of situational awareness were mentioned at least on a conceptual level.

Table 3: Number of identified papers that described functionalities supporting various levels of situational awareness

Level of situational understanding	Papers where the functionality appeared at least as a concept
SA1: perception	25
SA2: comprehension	24
SA3: projection	25
Metacognitive processes	11

For all the classical three levels of situational awareness (Ensley, 1995) there was equal amount of support in the described COPs of the papers and there was least amount of notions of the functionalities that support the metacognitive processes.

An example of a study that covered also the metacognitive processes is the one by Robertson (2014) where integrity measure on situational awareness was formed based on information security principles. Another example is the study by Masnica et al. (2021) where measure of information entropy was used as an index for credibility of situational awareness information. It is suggested that presenting of these measures and indices to the decision maker could support his or her metacognitive processing related to the situational awareness.

3.2 Second Literature Review on Cyber COP

The numeric results of the second literature review are presented in Figure 2.

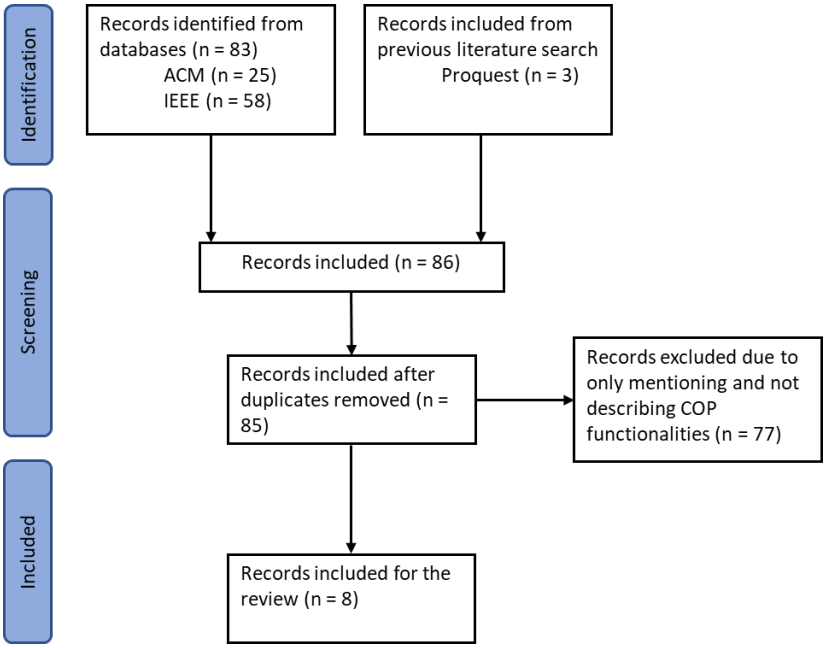

Figure 2: Result of the second literature review for cyber COP

For many of the selected papers it was difficult to define the actual level of management or warfare (tactical, operational, strategic) that they were targeted to. Either the issue was not clearly mentioned or it was difficult to infer based on the description. Despite these difficulties in interpretation, it could be said, that more than half of the selected papers (5 out of 8) covered cyber COP on the strategic level.

The readiness level of the concept or system described in each of the selected papers is presented in Table 4.

Table 4: The identified papers for each readiness level of the described cyber COP concept or application

Readiness level	Identified papers
1. Concept or list of user requirements	(Varga et al., 2018); (Coufalíková et al., 2021); (Pahi et al., 2017)
2. Working prototype	(Kaufhold et al., 2024); Llopis et al., 2018); (Cho e al., 2018); (Skopik et al., 2022);
3. Prototype that has been studied	(Noel et al., 2018)
4. In operative use	-

Based on analyzing the descriptions of the concepts and prototypes in the papers the relations of the reported (user) requirements or functionalities were categorized by which level of situational awareness they supported, following the Ensley's (1995) three level model with the added metacognitive processes.

Table 5: Number of identified papers that described functionalities supporting various levels of situational awareness

Level of situational understanding	Number of papers where the functionality appeared at least as a concept
SA1: perception	8
SA2: comprehension	8
SA3: projection	5
Metacognitive processes	1

The described information needs or functionalities for supporting the processing of third level of situational awareness (SA3), projection, were varied in the selected papers. Varga et al. (2018) surveyed information needs of government officials and employees of companies that operate with critical infrastructure. Regarding the process of projection (SA3) the respondents mentioned of a need to be aware of the temporal aspects of

the unfolding events, mentioning, for example, prognosis. Current status of the events was not considered sufficient, but there was also a need for prognosis about the restoring of the affected systems.

In the study by Llopis et al. (2018) there was comparison of two different prototype systems for presenting cyber COP. In the described VISA system there was included enemy behavioral modeling and a possibility to do "what if" projections of possible unveiling of events. The visualizations were based on nodes that represented cyber assets and the nodes could be viewed in 3D view to see their mission-attacker-controls triangles. In the other described prototype, the CYCOP, there was, rather similarly, a consequence analysis tool to aid in decision making. This was based on a 3D visualization representing georeferenced assets with a possibility to estimate the hypothetical threat level of the system in case a certain asset is affected by given incidents.

Coufalíková et al. (2021) mention in their conceptual paper data mining, machine learning, and AI as means for producing predictions of future developments and mention the predicting of the spreading of malicious code as an example of a use case for such functionality. Cho et al. (2018) analyze various cyber kill chain models in their paper and also present a cyber kill chain model that could be used in viewing of the cyber situational awareness. In the paper they shortly mention that a commander could make predictions on the threat in the form of an attack chain. And finally, Pahi et al. (2017) describe in their paper information types and sources that are needed for the supporting of a cyber COP. They go through categories of decisions that are done based on cyber COP and mention as a one category the decisions that have focus in the long term, such as even adapting relevant legislation.

Only in the paper by Kaufhold et al. (2024) there were notions about supporting the so-called metacognitive processes with the system design. In their design case study, they formed user requirements and design heuristics for a real-time cybersecurity dashboard. One of the listed user requirements was for the system to "evaluate information based on trustworthiness and provide data to the user for verification". Related design objectives were "links to the original source, displayed metadata, and traffic light indications for the verification of content".

4. Discussion

In the current study the relative extent of literature on cyber situational awareness compared to studies on situational awareness in other domains was examined. In addition, the aim was to examine within the previous studies on cyber COP how the functionalities supported the three levels of situational awareness and related metacognitive processes. In part, the motivation for the study was to see whether the suggestions of design guidelines for designing systems that support situational awareness have been followed.

In the first literature review for the COP systems in various domains it was observed that majority of previous studies described COP systems that were on conceptual level or lists of user requirements and there was lack of studies where effectiveness of COP systems and their designs would have been tested. Majority of previous studies were either in the army or in the cyber context. In addition, there were more studies with descriptions of functionalities supporting the three traditional levels of situational awareness (perception, understanding, projection) than there were studies describing functionalities supporting the metacognitive processes that are relevant for situational awareness. In the second literature review that was targeted to cyber COP, similar effect was observed in the readiness levels of the cyber COP systems described in the papers. That is, there was lack of studies that would have verified the effectiveness of described cyber COP systems in mediating and forming situational awareness. In addition, there was also least amount of studies on the functionalities that would support the metacognitive processes that are relevant for situational awareness.

It is suggested, that more research efforts should be targeted towards empirically verifying the effectiveness of different design and visualization solutions in building cyber situational awareness. In this effort, the guidelines for situationally aware design could be systematically tested and updated. In addition, also the studies on information visualization should be considered when forming possible new design guidelines (see, for example Dimara et al., 2018).

5. Ethics and AI Declaration

Ethical clearance was not required for the current research according to the national laws and regulations. No artificial intelligence (AI) tools were used when preparing this paper.

References

Cho, S., Han, I., Jeong, H., Kim, J., Koo, S., Oh, H., & Park, M. (2018, June). Cyber kill chain based threat taxonomy and its application on cyber common operational picture. In 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-8). IEEE.

Conti, G., Nelson, J., and Raymond, D. (2013, June). Towards a cyber common operating picture. In 2013 5th International Conference on Cyber Conflict (CYCON 2013), pp 1-17. IEEE.

Coufalíková, A., Klaban, I., Šlajs, T., & Štefek, A. (2021). Concept of Solution for Cyber Common Operational Picture Gaining. In 2021 Communication and Information Technologies (KIT) (pp. 1-4). IEEE.

Dimara, E., Franconeri, S., Plaisant, C., Bezerianos, A., and Dragicevic, P. (2018). A task-based taxonomy of cognitive biases for information visualization. *IEEE Transactions on Visualization and Computer Graphics*, Vol 26, No. 2, pp 1413-1432.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors,* Vol 37, No. 1, pp 32-64.

Endsley, M. R., and Jones, D. G. (2012). *Designing for Situation Awareness: An Approach to User-Centered Design*. Second Edition. CRC Press.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, Vol 46, pp 18-31.

Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., & Babar, M. A. (2022). Systematic literature review on cyber situational awareness visualizations. *IEEE Access*, Vol 10, pp 57525-57554.

Kaufhold, M. A., Riebe, T., Bayer, M., and Reuter, C. (2024). 'We Do Not Have the Capacity to Monitor All Media': A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams. In *Proceedings of the CHI Conference on Human Factors in Computing Systems,* pp 1-16.

Llopis, S., Hingant, J., Pérez, I., Esteve, M., Carvajal, F., Mees, W., and Debatty, T. (2018). A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. In 2018 International Conference on Military Communications and Information Systems (ICMCIS) (pp. 1-7). IEEE.

Masnica, R., & Štulrajter, J. (2021). Using a Probabilistic Model of Signal Processing in Technologies in Military Practice. In 2021 Communication and Information Technologies (KIT), pp 1-5. IEEE.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., and Prisma Group. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International Journal of Surgery*, Vol 8, No. 5, pp 336-341.

Noel, S., Rowe, P. D., Purdy, S., Limiero, M., Lu, T., and Mathews, W. (2018). Mission-focused cyber situational understanding via graph analytics. In 2018 10th International Conference on Cyber Conflict (CyCon), pp 427-448, IEEE.

Pahi, T., Leitner, M., and Skopik, F. (2017). Preparation, modelling, and visualisation of cyber common operating pictures for national cyber security centres. *Journal of Information Warfare*, Vol 16, No. 4, pp 26-40.

Robertson, J. (2014). Integrity of a common operating picture in military situational awareness. In 2014 Information Security for South Africa, pp 1-7. IEEE.

Rousseau, R., Tremblay, S., Banbury, S., Breton, R., and Guitouni, A. (2010). The role of meta-cognition in the relationship between objective and subjective measures of situation awareness. *Theoretical Issues in Ergonomics Science*, Vol 11, No. 1-2, pp 119-130.

Skopik, F., Bonitz, A., Grantz, V., and Göhler, G. (2022). From scattered data to actionable knowledge: Flexible cyber security reporting in the military domain. *International Journal of Information Security*, Vol 21, No. 6, pp 1323-1347.

Varga, S., Brynielsson, J., and Franke, U. (2018). Information requirements for national level cyber situational awareness. In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp 774-781. IEEE.

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, Vol 105, 102239.