Framework for Cognitive Warfare Situational Awareness Visualization

Mario Aragonés, MSc., Alfonso Climente, Ph.D.,
Israel Pérez, Ph.D., Manuel Esteve, Full Professor.
Distributed Real Time Systems LAB.
Universitat Politècnica de València
Camino de Vera, s.n. Valencia
SPAIN

mesteve@dcom.upv.es

ABSTRACT

Situational Awareness is defined as "The perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [1]. Situational awareness belongs to cognitive domain and it is related with perceptions, knowledge, mental models and training. On the other hand, Cognitive Warfare [2] belongs to cognitive world, obviously, and encompasses a broad range of elements including technical aspects but not limited to as it also relates to social and human facets. In nowadays environments and scenarios, where operations do have a multi-domain nature, cognitive domain is considered transversal to the other domains, mainly, the traditional kinetic or physical one, as well as the more recent cyber domain. Without a doubt, the cognitive domain is the more complete, encompassing and complex one regarding the situation perception due to its transversal and all-the-rest comprehending nature. Therefore, it will be needed the generation of a Situational Awareness (SA) integrated into the Cognitive Warfare scope that allows for conducting operations in the cognitive domain in a transversal manner with regards to the all other domains. It could be stated that the cyber space is the main battlefield for Cognitive Warfare. As a consequence, Cyber Situational Awareness generation constitutes the prior and mandatory step for Situational Awareness generation in the cognitive domain. It will also be a key component acting as a unifying thread in SA production due to its cross-cutting nature.

1.0 INTRODUCTION

Nowadays there are efforts to integrate in a unique and holistic Situational Awareness, objects belonging to cyber space and those belonging to the kinetic domain, whether they are coming them from land, maritime, air or space.

Aligned to the previous statement, the proposed Situational Awareness must be feed by sensed data coming from kinetic and cyber domains, as well as objects belonging to the psycho-social domain, such as cultural elements, aspects related to human behaviour, social networks and media in a broad sense. Although sensors and data sources for kinetic and cyber domains are precisely defined and bounded up to some extent, that is not the case for raw data

coming from the psycho-social domain, where strong efforts must be made to define a common agreement.

Besides, Situational Awareness visualization poses a relevant challenge and it constitutes an open research field, both for the kinetic and, even more, for the cyber domain [3], [4]. As a result, Situational Awareness visualization in the Cognitive Warfare domain is an extremely challenging field with very few efforts, if any, done so far in the academia and in the industry fields.

In this paper, an architecture or framework for Situational Awareness generation at cognitive level is proposed, inscribed in the Cognitive Warfare domain. The relation of the cognitive domain with others will be taken into account, paying special consideration to the intersection among different domains, with possible overlapping, that will lead to hybrid domains and the associated complexities that those domains provide in the Situational Awareness generation as basis for the decision-making process in a multi-domain environment.

The definition of the cognitive domain constituent and specific objects [5] will be an a priori step to be taken in the development of the Situational Awareness generation capability.

In addition, most significant aspects to be taken into account for the visualization of Cognitive Situational Awareness will be outlined. A first approach study on visualization techniques for Cognitive Warfare Situational Awareness will be sketched, paying attention to psychological and technical aspects such as the application of visual analytics techniques or the requirements in terms of complex multi-dimensional graphs generation.

2.0 COGNITIVE WARFARE SITUATIONAL AWARENESS FRAMEWORK

The cognitive domain has started to be considered as the sixth operational domain, alongside the physical domains (land, maritime, air and space) and the cyber space.

One of the objectives of the information systems for Command and Control is Situational Awareness generation per each of the before mentioned domains. Situational Awareness can be defined as "the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future".

Situational Awareness is a mental state and, regardless of the domain, it is generated as a cognitive capability.

This leads to a high increase in terms of complexity when defining or stating how to generate Situational Awareness at the cognitive domain, considering the cognitive domain as the operations domain.

First approach would be to consider that cognitive domain Situational Awareness must encompass the Situational Awareness of the other five domains.

A second approach would be to consider that cognitive domain Situational Awareness is based on information's plane, and it is generated from the hybridization of the physical and the cyber Situational Awareness, including the intrinsic psychological and social aspects belonging to the cognitive domain.

Next, a framework for the Cognitive Situational Awareness generation is proposed.

In Figure 1, the proposed architecture is shown. As we can see, Cognitive Situational Awareness is generated by means of the integration of:

1) Physical world Situational Awareness
2) Cyber space Situational Awareness
3) Psycho-social components of the interest area population.

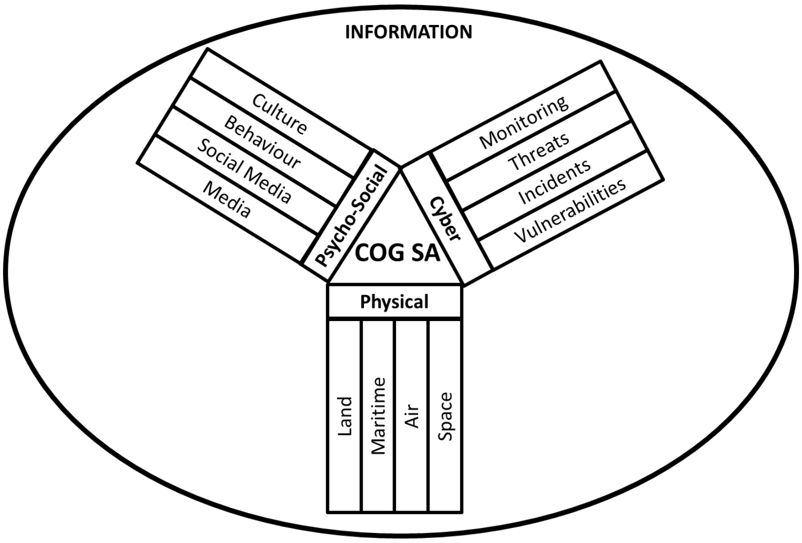

Figure 1. Cognitive Warfare Situational Awareness Framework.

Our proposal for the Cognitive Situational Awareness generation is oriented to the operational and tactical planes, that is it, it is not an abstract concept but an actionable concept, as supporting element in Decision Making in a multi-domain operations environment.

With this perspective, each of the Cognitive Situational Awareness components will be composed, in turn, by a series of elements or objects specific from the operations area.

2.1 Physical Situational Awareness

It will be composed by the integration of the different Situational Awareness: land, maritime, air and space Situational Awareness. Each domain’s Situational Awareness will be generated by the Command and Control information systems specific to each domain, with their own objects and elements.

One example of a tool for visualizing the multi domain situational awareness in joint operations is NATO’s NCOP.

2.2 Cyber Situational Awareness

The objects that do compose the cyber Situational awareness are the assets, vulnerabilities, threats, alarms, incidents and risk-related elements. At Cyber space, Situational Awareness is composed of three levels: network awareness, threat awareness and mission awareness. The relationships and interdependencies among those three levels are obtained from and are based on the risk analysis where the interdependencies among physical and logical components of the systems, services and the mission are defined.

Cyber situational awareness, following Endsley’s definition, does not encompass all of the cyberspace but focuses on the segment or volume of it which is relevant for the operations development and unfolding, known as cyber key terrain.

2.3 Psycho-Social Components

Not being exhaustive, we can point out the following main psycho-social domain components: cultural aspects, population’s behaviour at the operations theatre area, mass media involved in generating public opinion and social media.

Special relevance does have the social media, particularly social networks, as the generation of their contents depends on the most individual and psychological aspects of the cognitive domain, but, at the same time, they do contribute to the generation of the social dimension of the cognitive domain.

It must be highlighted that, for the production of the cognitive Situational Awareness, only psycho-social components of population in the operations' interest area will be considered.

3.0 THE COGNITIVE SITUATIONAL AWARENESS VISUALIZATION ACTIONABLE APPROACH

From the authors' point of view, Cognitive Situational Awareness visualization must have as goal the enhancement of the decision making process in joint operations.

In many nations, the operations in the cognitive domain, planned and conducted in order to produce effects at the other domains are known as "information operations".

Previously cited information operations do have, as objective, on one hand side, to create an opinion state that could be named "cognitive state" in the cognitive situational awareness domain or, on the other hand, are devoted to counteract the adversarial information operations, which, from a self-perspective could be seen as deception or disinformation operations.

In the information age, within a multi-domain environment, most of the operations at the cognitive domain, whether they are information or deception operations, are based mainly in the capabilities that the fifth domain, cyber space, does provide. Specifically, those capabilities relay on the capillarity and the exponential information diffusion capability of the social networks.

Previous statement does not necessarily imply that we have to get rid of the capabilities provided by the traditional communication means, mainly TV due to the massively distributed image power, which many times produces a multiplying effect on the information generated and spread using the social networks.

Then, an actionable application of the visualization capabilities of the cognitive situational awareness could be the evaluation of the opinion state of the population of interest, before and after triggering an information operation, to verify the effect of the given operation.

To do so, the best way to carry the described evaluation could be by means of social networks contents monitoring and correlation of the target population of the information operation, before and time after the conduction the operation.

A tool to generate the Cognitive Situational Awareness with that given goal in mind, should have capabilities of social networks contents acquisition, correlation of those contents following a given set of criteria defined by the analyst and raw data sources visualization, as well as and more importantly to achieve the designed goal, the visualization of the correlations results.

Visualization of the cognitive domain is a challenging task. In fact, there is few to no literature in the State-Of-the-Art (SoA) and even it can be seen that, a lesser complex visualization domain such as cyber SA visualization is still an open research field where there are several very relevant efforts [6], [7] but where no consensus or agreement has yet been achieved. Worse, therefore, are things for Cognitive SA visualization, where, as was stated, very few works tackle the visualization aspects of this domain, and in a very remote way, such as [8].

From an intelligence point of view, a tool with such cognitive situational awareness visualization capabilities, could be considered as an OSINT (Open source Intelligence) tool, zero-intrusive, and with strictly bounded to existing legal frames for the target population.

On the other hand, results obtained for social networks monitoring must be correlated with other information sources related to the target population cultural environment, for instance, religion, ethnicity at multi ethnic societies, or the wealth and income level of individuals. This information can be mostly gathered from open sources by means of OSINT techniques. The correlation of these contextual information with real-time data acquired from social networks, dramatically enriches the Cognitive Situational Awareness. Examples of this kind of approaches can be seen in [9], [10].

It must be analysed which types of graphs and charts allow efficient visualization (and enable, also, the generation of the proper perceptions at the cognitive level), both for raw data sources and for the correlations results. Georeferenced heatmaps of the bubble aggregation diagrams, in conjunction with the traditional pie or bar charts, can help in generating the convenient Cognitive Situational Awareness.

In Figure 2, georeferenced OSINT data is shown as an example of its contribution to the overall Cognitive Warfare SA generation.

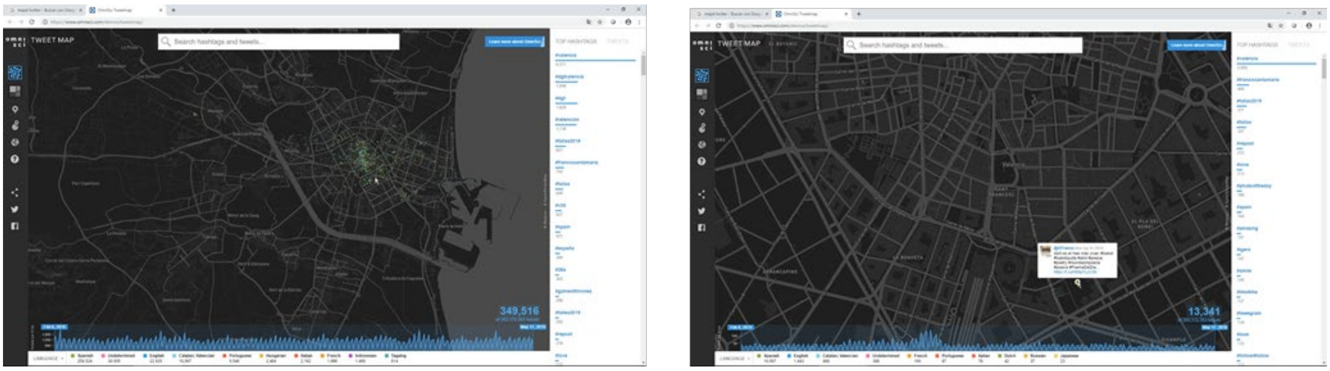

Figure 2. Open Source Intelligence contribution example 1 to Cognitive Warfare SA.

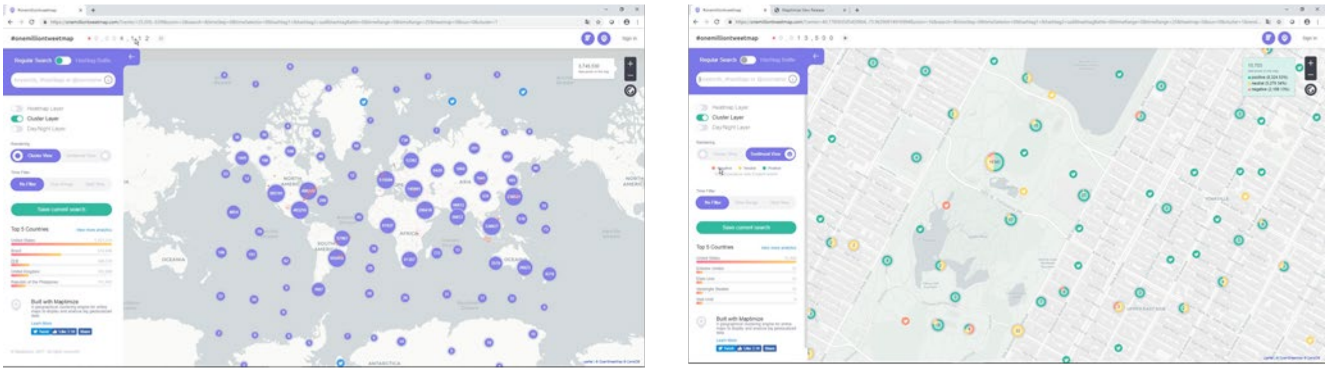

Figure 3. Open Source Intelligence contribution example 2 to Cognitive Warfare SA.

In Figure 3, an example of the geographical distribution of events in a given social network is shown. Cultural aspects (for instance the ‘sentiment analysis’ based on language automated processing) are taken into account for conducting Cognitive Warfare SA.

Usually, the most effective technological mean or environment to develop information and deception campaigns is cyber space. From the military perspective, the cyberspace is a domain where, as it happens at the kinetic domains, defensive, exploratory and offensive operations can be conducted.

Disinformation of deception campaigns can be considered as offensive operations in the cyber space. They can be implemented in a similar way as the distributed Denial of Service Attacks (DDoS), making use of thousands or millions of bots, cyber bots in this case.

Therefore, the inclusion of the Cyber Situational Awareness as a component to generate the Cognitive Situational Awareness, undoubtedly enriches the later. The tools that allow for the generation and visualization of the Cognitive Situational Awareness must provide correlation capabilities among sources from cyber space and from psycho-social, as well as the contextual information of the cultural scope of the target populations.

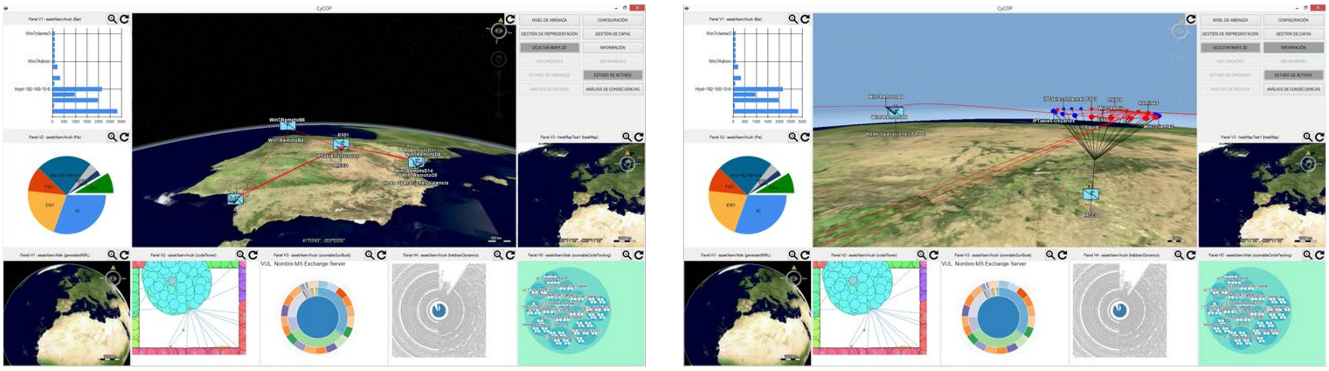

Figure 4. Physical and Cyber domain contribution examples to Cognitive Warfare SA.

In Figure 4, purely kinetic aspects as well as cyber domain exclusively aspects, besides their hybridization or the multi-modal view are shown or considered to be used as components of the Cognitive Warfare SA.

Lastly, operations at the cognitive domain could be classified as:

- **a)** Operations with effects only at the cognitive domain.
- **b)** Operations with effects at the cognitive domain and the kinetic domains.

In the latter case, cognitive situational awareness is not complete until the physical or kinetic situational awareness is included, to properly evaluate the effects that operations in the cognitive domain do produce at the kinetic domains.

On the other hand, it is clear that operations at the kinetic domains produce effects at the cognitive domain. Possibly, this aspect is historically the best-known and evaluated one. A Cognitive Situational Awareness tool must be capable of allowing the visualization of the effects that the kinetic operations produce at the cognitive domain.

Anyway, such tool should allow also the correlation of the effects that the cognitive domain operations do produce in the kinetic domain (for instance civil insurrections, uprisings or population displacements), as well as the effects that the operations in the kinetic domain do produce in the cognitive domain, for instance, the creation of states of mind about ‘good’ and ‘bad’ sides in a confrontation.

4.0 CASES OF STUDY PRELIMINARY ANALYSIS

Two clear examples on the interaction between the cognitive domain and the kinetic domains are the Ukraine invasion by the Russian Federation in 2022 and the war set off in Gaza after the jihadist organization Hamas incursion in Israeli territory October the 7th 2023.

In the former, the attacked contender acquires a prompt and continuous superiority in the cognitive domain as the Ukrainians are the good fellows in the story and western countries and their public opinions support and trust Ukraine.

In the later, the evidently attacked contender, Israel, loses the initial superiority in the cognitive field as per victim, that is, shortly after conduction kinetic operations in Gaza strip as a reaction to the attack, they lose the 'good guys' tag, as well as the 'complete trust' from 'all' the western countries and 'all' their public opinion.

What are the differences from one example to the other? No doubt that explanations must be found in other components beyond the kinetic military operations themselves. Reasons must be found in components from the cognitive situational awareness, mainly in psycho-social components as cultural aspects, religious, economical and from smart mass media tweaking, even tampering, both at traditional ones and at those based on social networks.

If only images from victims of one of the contenders are shown, very quickly superiority at the cognitive domain will fall on one side, the one with those victims in biased exposition of facts.

If NGOs and other organizations presumably neutral, only report inappropriate activities from one of the contenders, its influence in public opinion, and in trust, which we must remind that is the target of the cognitive domain, will opt for very quickly the superiority at the cognitive domain to the contender benefited by their biased complaints.

Without a doubt, a tool that could allow the visualization of the cognitive state of the different audiences in conflicts as those shown before as example, that permitted the assessment of the effect that operations in one domain produce in the other domains, and overall, in the cognitive domain, would be very useful to help in the decision-making process in multi-domain operations.

Potential audiences would be, for instance, Chiefs of Defense Staff of the contenders, public opinion of the nations or groups in dispute, third-party nations' public opinion (for instance western countries in the Ukraine-Russian Federation conflict or in the Israel-Hamas conflict) and, in general, policy makers of all the involved actors including third-party nations.

5.0 CONCLUSSIONS AND LOOKING AHEAD

A preliminary framework for the Cognitive Warfare Situational Awareness has been defined from a multi-domain perspective, taking into account three key contributions to generate the Situational Awareness: kinetic domains, the cyber domain and the psycho-social domain.

In our framework, we do understand that Cognitive Warfare Situational Awareness is based on the integration and correlation of those three components with their corresponding subcomponents.

So far, UPV has developed a complete knowledge in the integration of the kinetic and cyber domains, resulting in a hybrid or multi-domain Situational Awareness tool, CyCOP (Cyber Common Operational Picture) [11], [12], [13], currently in usage by the Spanish Cyber Command.

Next step will be to develop a prototype that will integrate the psycho-social components defined in the proposed architecture at this work, in order to validate the proposed model.

The tool will include the integration of OSINT sources, particularly social networks and other intelligence sources related to the sociological, economic, cultural and even religious (cultural awareness) environments of the populations at the areas under analysis.

The visualization of the analysis results is a challenging aspect, as well as the definition of the different views at the Cognitive Situational Awareness, depending on the target audience towards will be directed the tool usage.

6.0 REFERENCES

[1] M. R. Endsley and E. S. Connors, "Situation awareness: State of the art," 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 2008, pp. 1-4, doi: 10.1109/PES.2008.4596937.

[2] B. Claverie, B. Prebot, N. Buchler, D. du Cluzel, Eds, "Cognitive Warfare: First NATO scientific meeting on Cognitive Warfare", Bordeaux, France, June 2021.

[3] Heer J and Shneiderman B. Interactive dynamics for visual analysis. Commun ACM 2012; 55: 45–54.

[4] Jia et al. "Systematic literature review on cyber situational awareness visualizations", IEEE Access, 2022.

[5] C. Perring, 'Wargaming elections interference: A serious influence game for teaching elements of cognitive warfare', Dissertation, 2022.

[6] Eslami et al., "Deriving cyber use cases from graph projections of cyber data represented as bipartite graphs", IEEE International Conference on Big Data, 2017.

[7] Kullman et al., "Enhancing cyber defense situational awareness using 3D visualizations", International Conference on Cyber Warfare and Security, 2018.

[8] Gilles Desclaux. Trust Between Humans and Intelligent Machines and Induced Cognitive Biases. Bernard Claverie; Baptiste Prébot; Norbou Buchler; François du Cluzel. Cognitive Warfare: The Future of Cognitive Dominance, pp.5, 1-5, 2022. 978-92-837-2392-9. hal-03635913

[9] Gianluigi, M. E., & MUCCI, M. F. (2023, May). Countering Daesh Cognitive and Cyber Warfare with OSINT and Basic Data Mining Tools. In International Conference on Cybersecurity and Cybercrime. Vol. 10, pp. 71-80.

[10] Casanovas, P. (2017). Cyber warfare and organised crime. A regulatory model and meta-model for open source intelligence (OSINT). Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative, 139-167.

[11] Esteve, M.; Pérez, I.; Palau, C.; Carvajal, F.; Hingant, J.; Fresneda, M.A.; Sierra, J.P. Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement; Technical Report STO-MP-IST-148; North Atlantic Treaty Organization (NATO), Science and Technology Organization (STO): Brussels, Belgium, 2016.

[12] Llopis, S.; Hingant, J.; Pérez, I.; Esteve, M.; Carvajal, F.; Mees, W.; Debatty, T. A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. In Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, 22–23 May 2018; pp. 1–7.

[13] Kim, K.; Youn, J.; Yoon, S.; Kang, J.; Kim, K.; Shin, D. Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness. Appl. Sci. 2023, 13, 2331.