Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement

Manuel Esteve / Israel Pérez / Carlos Palau / Federico Carvajal/ Javier Hingant
D. Comunicaciones. Universitat Politècnica de Valencia
Camino de Vera S/N, Valencia 46022
SPAIN

mesteve@dcom.upv.es / ispello0@upv.es / cpalau@dcom.upv.es / fecarrod@upv.es / jahingme@upv.es

Miguel A. Fresneda / Juan P. Sierra
Spanish Joint Cybercommand
Base de Retamares, Ctra. de Boadilla del Monte, km 3.4
28223 Pozuelo de Alarcón, Madrid
SPAIN

mfremor@et.mde.es / jsielor@oc.mde.es

ABSTRACT

Remote firewall management, Intrusion Detection Systems (IDS), etc. are part of cyber defence and of Cyber Command and Control Systems but, are not in themselves or do not constitute exclusively the Command and Control system. To develop strategies and tactics in the cyber defence domain it is required something else: a true information system for command and control which integrates the three traditional battlefields, space and cyber space, cross-cutting, in a unique decision-making space based on the proper commander's Situational Awareness (SA). Cyber Common Operational Picture (CyCOP), is a tool developed by Universitat Politècnica de Valencia in collaboration with the Spanish Joint Cybercommand and Spanish Ministry of Defence (DGAM) whose objective is to generate the Cyber Hybrid Situational Awareness (CyHSA). The application core is the fusion module which fuses cyber domain information (threats, attacks, vulnerabilities and so on) obtained by 'traditional' means (sensors, SIEM) with georeferenced information from physical domain command and control systems. As most relevant perception organ is sight, and based on it situation perception is mostly generated, visualization aspects will be taken into account, allowing the transition from one kind of visualization to others, depending on the decision-making scope: strategic, operational or tactical/technical. In the present paper CyCOP development motivation will be presented, its justification in the field of Cyber Situational Awareness (CySA), as well as an approach to the tool's architecture.

1.0 INTRODUCTION

Only very recently has cyber space been addressed as another battlefield, jointly with land, maritime, air and space theatres.

Security platforms for networking and information systems have been considered up to now as a collection of components, firewalls, antivirus, scanners, IDS, etc. whose main aim was to provide security to the information systems in a preventive or passive manner.

Traditionally those devices proceed by generating messages that receive and process a human operator. In more complete systems, those visualization techniques that provide a better perception to the operator are taken into account. In any case, cyber security systems visualization is a research field still open and not yet

fully solved.

However, those systems are designed for limited-scale attacks, done for economic interests or most of the times just due to intruder's self-challenge. They are not conceived for a massive attack to critical systems with the aim of collapsing a nation or at least some of its infrastructures.

The innovative character of CyCOP as a CySA visualization tool is that it has the features of a military Situational Awareness application, allowing operation's commanders to jointly perceive the situation in the land, sea, air, space and cyber space domains as a unique "integrated battlefield" and decision-making scope as decisions taken in any of them influences the remaining.

CyCOP takes into account strategic, operational and tactical/technical levels when presenting the information.

Differences when conducting operations in physical and cyberspace are evident. First, there is the pace and progression of events. Physical spaces Command and Control systems (Kinetic C2) are developed, each one on its scope, to obtain proper Common Operational Picture (COP) in useful time regarding that particular scope. This useful time can be minutes or even hours. However, useful time to gather COP as a support to conduct operations in cyber space can be estimated in seconds, but taking into account that cyber events influence in real systems is nearly immediate.

Hence, among other things, the military need to face the joint COP generation, considering cyber space operations as "security and protection operations" over the physical world operations (Kinetics operations).

2.0 STATE OF THE ART IN CYBER SITUATIONAL AWARENESS

In specialized literature there are several efforts related to the goal to be achieved with CyCOP, nevertheless the authors consider that, mainly from the military point of view, the hybrid CySA approach proposed goes one step beyond of existing approaches.

In "A Cyberspace Command and Control Model" (Scherrer and Grund, USAF Air War College, 2009) [1] authors deeply argue the need to conduct joint operations in land, maritime, air and cyber space theatres.

In "Cyber situational awareness - A systematic review of the literature" (Franke and Brynnielsson, Elsevier Computers and Security, 2014) [2] the most recent summary about works on CySA can be found.

In "Toward a Model-Based Cyber Defence Situational Awareness Visualization Environment" (Klein et alt., RTO-MP-IST-093) [3] traditional visualization techniques in cyber security systems are tackled stating their inefficiency to obtain the proper CySA in military domains.

Some advances in visualization are proposed aimed at integrating over a traditional interface geo referenced information about cyber events. Finally, cyber security information translation is proposed, integrated with command and control information by means of the usage of a user interface based on graphs with nodes, links and dependencies among them.

In "A Multi-Level Analysis Framework in Network Security Situation Awareness" (Zhang et alt., Elsevier Computer Science, 2013) [4] an interesting model to identify the values/events that contribute to the CySA generation is proposed, as well as for the application of correlation rules which, starting from the current situation assessment (in our case the hybrid situation) allow the foreseen of its future evolution.

In "VACS: Visual Analytics Suite for Cyber Security - Visual Exploration of Cyber Security Datasets" (F. Fischer, D. Keim, IEEE VIS 2013) [5] most proper visualization techniques for a cyber security environment

are studied paying attention on the importance of the enhancement they provide to users situational awareness.

In "A Survey of Visual Analytics Techniques and Applications: State-of-the-Art Research and Future Challenges" (Guo-Dao Sun, Rong-Hua Liang, Shi-Xia Liu, Elsevier Journal of Computer Science and technology, 2013) [6] an exhaustive survey on most recent 'visual analytics' techniques and their applications is done, particularly in the cyber defence domain.

In "Spherical layout and rendering methods for immersive graph visualization", (Oh-Hyun Kwon, Chris Muelder, Kyungwon Lee, Kwan-Liu Ma, IEEE Pacific Visualization Symposium (PacificVis), 2015) [7] techniques for efficient representation of graphs in immersive environments are highlighted.

A similar work, but applied to the representation of collaborative environments in social networks is shown in "GraphiteVR: A Collaborative Untethered Virtual Reality Environment for Interactive Social Network Visualization" (S. Royston, C. DeFanti, K. Perlin, IEEE Scientific Visualization (SciVis) Conference, 2016) [8].

All this precedent work face partial aspects of CySA elaboration, however, it is needed the integration of all them in a holistic approach. Moreover, other aspects not related in this short summary of prior work are needed to obtain a real CyHSA as it is the goal of CyCOP.

Last, we should mention the FP7 project PANOPTESEC [9][10] where, among others, the generation and visualization of CySA in non-military systems is faced, not considering the idea of a joint cyber COP. However, the Project highlights the interest in the matter at different forums such as European Commission in the area of information security.

3.0 CYBER SITUATIONAL AWARENESS, CYBER COMMON OPERATIONAL PICTURE AND CYBER HYBRID SITUATIONAL AWARENESS.

Starting from the traditional concept of Situational Awareness:

"Situation awareness is 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."[11]

Cyber Situational Awareness allows for current situation understanding and helps commanders in the process of decision making:

"Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, competitive and other operations within the battlespace in order to facilitate decision making. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding." [12]

CyCOP novelty is the battle-space uniqueness by means of the integration of a COP of prior knowledge and incoming events as a result of the five stated spaces real-time monitoring.

Lastly, the traditional definition of Situation Understanding will be projected as the capability to predict future courses of operations, again in a unique decision making space.

"Understanding involves having a sufficient level of knowledge to be able to draw inferences about the possible consequences of the situation, as well as sufficient awareness of the situation ***to predict future***

***patterns**."*[13]

Making use of graph and complexity theory, the three traditional spaces, space plus cyber space will be represented as unique decision making space that, based on physical systems (land, air, maritime and space COP) nodes and links georeferencing will give way to a multi-dimensional "cyber referencing" allowing the conduction of operations (cyber command and control) in this unique space.

The advanced concept of Cyber Hybrid Situation Awareness (CyHSA) is clearly implemented in CyCOP, allowing for commanders' inference of the effects of an event in a given plane onto the other planes.

Current hybrid real situation, presented as CyHSA, will be derived from a known initial situation based on logical and physical elements, combined with changes occurred during operations course reported by physical world C2IS and by data/events reported by security elements at cyber space.

To analyse incoming data/events, from any plane, a two-phase processing will be applied:

- Data/event identification
- Relation rules application between data/events

This two-phase analysis entails that each incoming data type (coming from land, maritime, air, space or cyber spaces) will be addressed by a process which will apply corresponding user-defined relation rules. So, for instance, an event such as "lost link with a vehicle (and therefore lack of knowledge of its current geolocation)" will influence the associated node representation and also the representation of the rest of nodes linked to it, Another example: a service denial cyber space attack to a video server will be influential to the analysis capabilities of the intelligence nodes that relayed on that video server.

With this two-phase processing we go beyond the SA concept, allowing for effects inference that for the future course of operations will have an incoming data/event.

4.0 HMI AND VISUALIZATION OF CYBER HYBRID SITUATIONAL AWARENESS

Given that main perception organ is vision and upon it situation perception is mainly based on, visualization aspects will be very present, allowing for the transition between different representations. For instance:

- Georeferenced map with regards to logic system location
- Cyber referenced map with regards to physical system cyber location
- Dependencies between logical and physical systems visualization
- Operator-selected granularity of an area of interest

The visualization system, as well as the icons and codes used should be oriented to highlight anomalies, as they are better detected perceptively. The final goal is the visualization of dependencies among physical and logical systems.

The granularity level and kind of representation for an area of interest will be user selected, depending on the CyHSA visualization level: strategical, operational or tactical/technical.

CyCOP provides, as a novelty, the implementation of advanced CyHSA visualization techniques, making use of:

- 3D Models
- Virtual Reality
- Immersive virtual reality

Depending on the application or the on-going mission, operators will select or commute from one visualization to another.

In figure 4-1, CyCOP HMI general structure schema is shown:

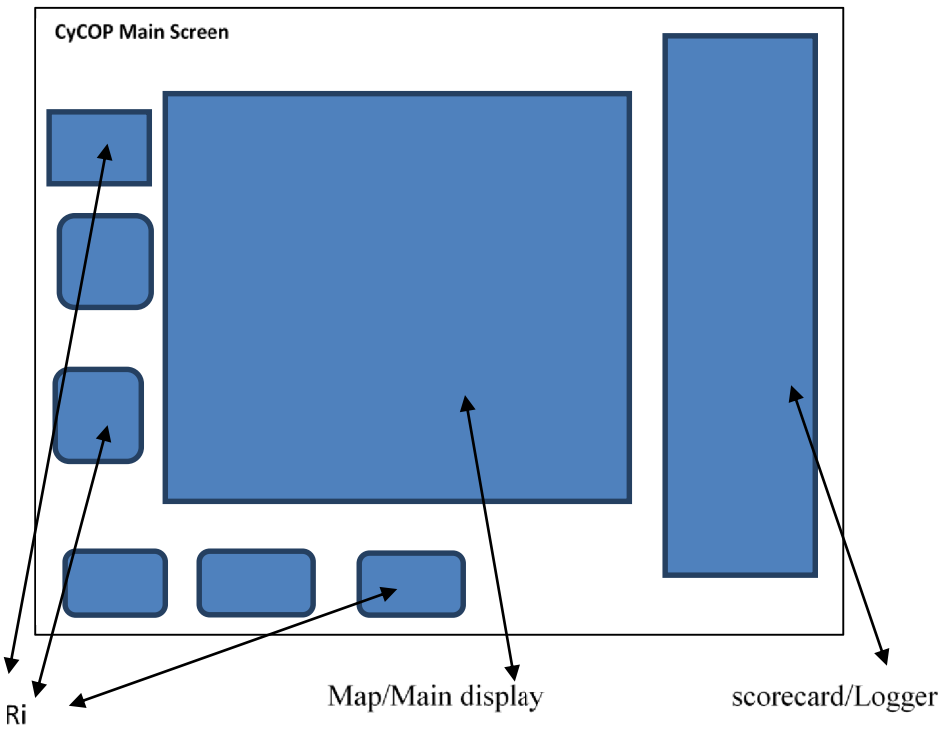

Figure 4-1: CyCOP HMI general structure.

At the main representation/map operators can see: only the C2 domain, only the cyber domain, hybrid C2 or combined C2 and cyber in two screens filling up the main representation. The scorecard/logger area provides further controls for the user to interact with the system as well as a detail level configurable log of the actions taken by the user and main events occurred. On the other hand, R_i areas stand for on-the-fly generated data representations when requested by users, using advanced, cognitive loop enhancing techniques such as dendograms, stream graphs, hive plots, etc. as well as classical representations such as pie or bar charts and step line.

CyCOP provides also an interface to activate communication with different external sources, for instance, activate communication with a SIEM (Security Information and Event Management) and within it to obtain assets, alarms, etc.

Assets insertion interface allows:

- Automatic insertion by means of connection to and retrieving from external SIEMs
- Manual insertion by operators

- Association of aspects from the physical world to previously inserted assets in the cyber domain, such as associated unit, affiliation, GPS position or sensors.

.

In figure 4-2 it can be seen an example of strategic level representation. In this example, it can be seen that the system uses the layout described at Figure 4-1 where there were several representations Ri (pie chart, hive plots, word clouds, etc.) on the left and bottom part, a central GIS representation of information and a scorecard/logger on the right side.

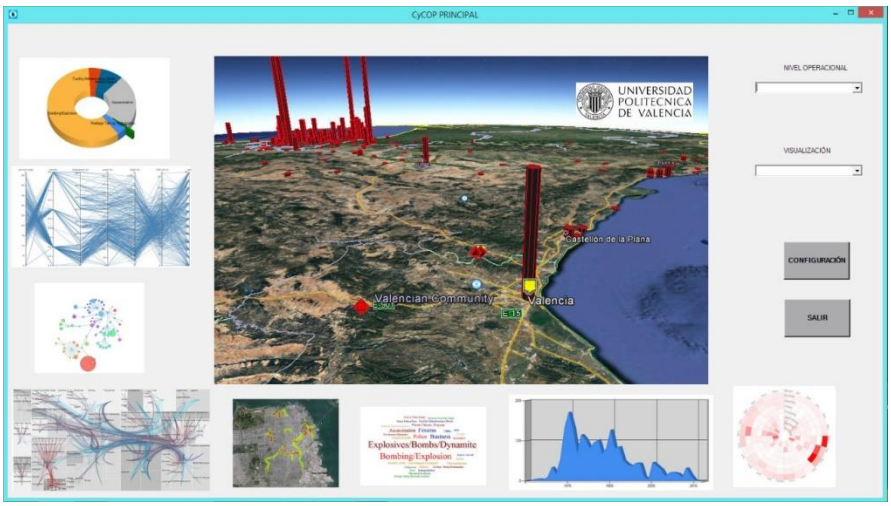

Figure 4-2: CyCOP strategic level representation.

Finally, an innovative contribution of CyCOP is the immersive virtual reality visualization capability. In this case, physical requirements of the system are at least:

- 64-bit, double core, 3 GHz processor
- RAM: 8 GB
- Hard Disk: 2 TB
- Graphics card: nVidia 970 or higher
- Immersive virtual reality glasses: Oculus Rift DK2 glasses with OLED display, accelerometer, gyroscope and magnetometer

The objective is to obtain visualizations similar to the one shown at figure 4-3, but inside an immersive environment where the operator can switch planes “from inside” the representation, thus understanding much better the relation among different planes. In the visualization we can see a 3-D view of the relationships between vulnerabilities, assets and nodes for a given threat.

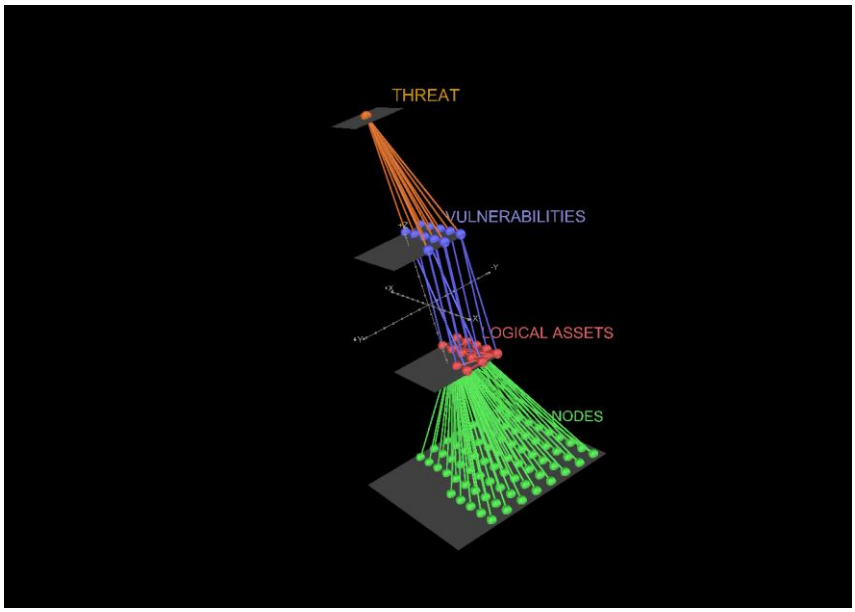

Figure 4-3: Immersive graph representation.

A priori, this kind of representation seems to be more suited to operational level visualizations but can be used at the other levels: the aim is to see "things" that cannot be seen in other kinds of representations, above all relations between different plane assets.

5.0 CYCOP ARCHITECTURE

In figure 5-1 CyCOP architecture is shown:

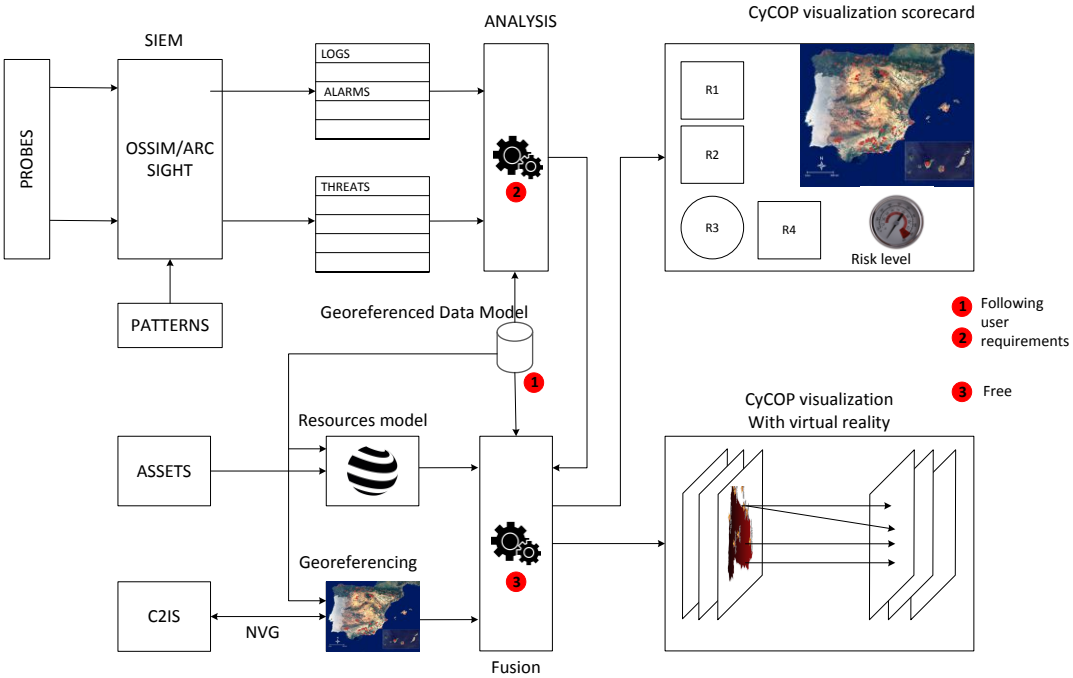

Figure 5-1: CyCOP architecture.

As can be seen, CyCOP gathers information from several external cyber systems (such as OSSIM, MISP and others) as well as C2 systems and fuses and stores it in a data model that constitutes system's core. With this information, cyber, physical and hybrid situation awareness can be generated, as well as on-demand advanced visualizations. On the other hand, immersive virtual reality visualizations that enhance SA are considered.

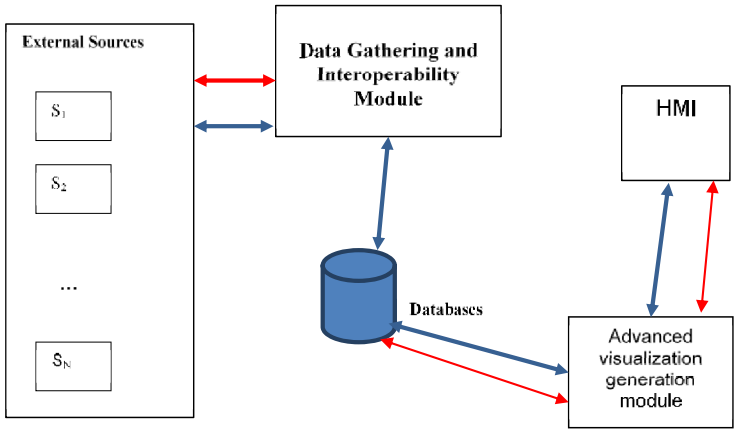

Figure 5-2: Interaction modes.

As can be seen in figure 5-2, CyCOP system obtains information from several external sources to feed its data model through the data gathering and interoperability module. This information can be obtained in a periodic and automatic way, without user's intervention (blue lines) or asynchronously on-demand (red lines). This includes both the communication with cyber systems and C2 systems and even bidirectional. On the other hand, visualizations generation will be in most cases on demand but there will be an automatic periodic process that will generate a basic visualization (basic COP on map or cyber).

Following most relevant CyCOP use cases are detailed.

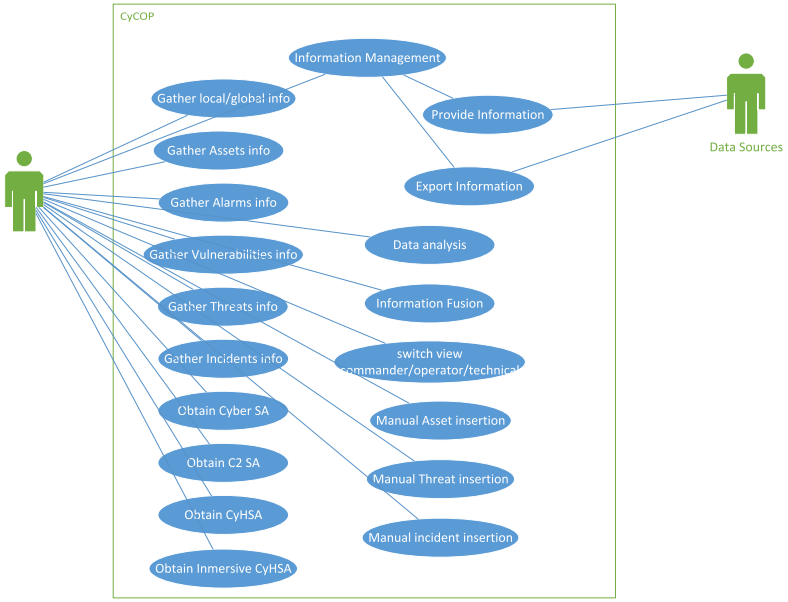

Figure 5-3: CyCOP use cases.

As we can see in Figure 5-3, there are 6 main categories of actions: automatic information gathering from its sources, obtain Situational Awareness (Cyber, C2 or hybrid), switch usage mode, data analysis actions, data export and manual data insertion.

6.0 CONCLUSIONS

A first approach to CyCOP tool and its motivation, main goals and high level architecture has been presented.

We base the design and implementation of CyCOP on the assumption that traditional battle field spaces (land, maritime, air and space) are closely connected with the cyber space new battle field. Other important assumption is that attacks or incidents that emerge in a space have strong influence in the other spaces. Particularly in case of attacks/incidents in the cyber domain that will influence over the security and operativeness of elements at the physical domain.

CyCOP is a CySA tool that allows for operations conduction taking into account both the physical and cyber planes, and above all their interrelations, generating the proper Cyber Hybrid Situational Awareness at strategical, operational and tactical levels.

Visualization is key aspect in CyCOP in order to provide proper CyHSA to commanders on duty at operations, as well as helping technical staff work involved on them.

CyCOP provides different kinds of visualization depending on the level we want to provide CyHSA: strategical, operational or tactical/technical. And ranges from traditional visual representation techniques (such as bar plots, pie charts and so on) to more advanced methods as chord diagrams or nested tree maps or even most advanced methods based on immersive virtual reality techniques.

7.0 REFERENCES

[1] J.H Scherrer, W.C Grund, USAF Air War College, “A Cyberspace Command and Control Model”, 2009

[2] U. Franke, J. Brynnielsson, “Cyber situational awareness - A systematic review of the literature”, Elsevier Computers and Security, 2014

[3] Klein et al., “Toward a Model-Based Cyber Defence Situational Awareness Visualization Environment”, NATO RTO-MP-IST-093, 2012

[4] Zhang et al, “A Multi-Level Analysis Framework in Network Security Situation Awareness”, Elsevier Computer Science, 2013

[5] F. Fischer, D. Keim, “VACS: Visual Analytics Suite for Cyber Security - Visual Exploration of Cyber Security Datasets”, IEEE VIS 2013

[6] Guo-Dao Sun, Rong-Hua Liang, Shi-Xia Liu, “A Survey of Visual Analytics Techniques and Applications: State-of-the-Art Research and Future Challenges”, Elsevier Journal of Computer Science and technology, 2013

[7] Oh-Hyun Kwon, Chris Muelder, Kyungwon Lee, Kwan-Liu Ma , "Spherical layout and rendering methods for immersive graph visualization", IEEE Pacific Visualization Symposium (PacificVis), 2015

[8] S. Royston, C. DeFanti, K. Perlin, "GraphiteVR: A Collaborative Untethered Virtual Reality Environment for Interactive Social Network Visualization", IEEE Scientific Visualization (SciVis) Conference, 2016

[9] http://www.panoptesec.eu/

[10] M. Angelini, D. De Santis, G. Santucci, “Toward Geographical Visualizations for Hierarchical Security Data”, IEEE Symposium on Visualization for Cybersecurity (Vizsec), 2014

[11] M.R Endsley, “Toward a theory of situational awareness in dynamic systems”, Human Factors and Ergonomic Society, 37, 32-64, 1995

[12] United States Army Field Manual 1-02, September 2004

[13] D.S Alberts, J. J Garstka, R. E Hayes and D. A Signori, “Understanding Information Age Warfare”, CCRP Publication Series, August 2001