2018 International Conference on Military Communications and Information Systems (ICMCIS)

A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military

Salvador Llopis, Javier Hingant, Israel Pérez,
Manuel Esteve, Federico Carvajal
Departamento de Comunicaciones
Universitat Politècnica de València
Valencia, Spain

Wim Mees, Thibault Debatty
Royal Military Academy
Brussels, Belgium

***Abstract*—Starting from a common fictional scenario, simulated data sources and a set of measurements will feed two different visualization techniques with the aim to make a comparative analysis. Both visualization techniques described in this paper use the operational picture concept, deemed as the most appropriate tool for military commanders and their staff to achieve cyber situational awareness and to understand the cyber defence implications in operations. Cyber Common Operational Picture (CyCOP) is a tool developed by Universitat Politècnica de València in collaboration with the Spanish Ministry of Defence whose objective is to generate the Cyber Hybrid Situational Awareness (CyHSA). Royal Military Academy in Belgium developed a 3D Operational Picture able to display mission critical elements intuitively using a priori defined domain-knowledge. A comparative analysis will assist researchers in their way to progress solutions and implementation aspects.**

Keywords—*cyber defense situational awareness; security metrics; operational picture; 3D visualization*

I. INTRODUCTION

A comprehensive cyber situational awareness solution must be supported by visual means to assist operators for technical matters such as incident handling and military commanders for decision-making. The views produced may represent technical information or mission relevant data both separately or jointly. The authors´ research seek to exercise if different types of existing visualisation approaches may lead to different levels of cyber situation comprehension and understanding. Complementarity aspects are highlighted to learn about further implications in an implementation process. It certainly depends on which cyber elements are displayed and how the information depicted in pictures matches with the user needs. When operators and military commanders are confronted with stressful situations which demand rapid response actions, the perceived reality on the screen may vary due to the human nature, experience and skills. The challenge here is how to approach meaningful visualisation techniques able to maximize the operator's awareness especially when a cyber-attack occurs. The maximum awareness threshold is called "ground truth" which comprises the most accurate facts collected from the real world. Apart from the inherent human-related factors, which are subject of cognitive science, the technology dimension is playing a predominant role in providing the visual tools for network defenders or for decision makers in a situation centre.

Key questions are raised when developing a visualisation technique based on an overarching cyberdefence framework: (1) how to fulfil user visualisation requirements with regards to the tasks to be performed and (2) which technologies suit best this performance. A long iterative process is foreseen to tailor the operators' needs in the military field. Moreover, the engineering aspects of a possible architecture shall include data connectors with various sources, a mechanism to process the information and a decision-support system.

II. FICTIONAL SCENARIO

The following items describe a generic fictional scenario from which to derive and generate the required data and conditions applicable to the visualisation context.

A. Operational Setting.

In the framework of a given deployment of military nodes within a territory, a mission network (MINET) is established to ensure the Command and Control (C2) of the nodes. MINET is a Wide Area Network (WAN) where all the stakeholders can interoperate including non-governmental agencies and organizations acting as external users. The scenario is composed of physical nodes and cyber elements associated to each of them. The physical nodes are graphically referenced using a pre-defined Geographical Information System (GIS). Every node has its own associated cyber elements (hereafter assets) which can be routers, servers, desktop clients, laptops, etc. The association of assets to nodes (which node the asset belongs to) is facilitated by a tool. In this context, one of the services provided by the network is a common operational picture (COP) of the operational environment in the area of responsibility. This network relies on the commitment of the stakeholders, mutual trust and the accomplishment of agreed security policies. Malicious actors attempt to launch a campaign of cyber activities to disrupt the MINET. MINET includes different nodes for the units "Nodo Madrid", "Nodo Operaciones Ferrol", and "Nodo Operaciones Rota" and "Nodo Operaciones Valencia" located at various points of presence in the area of responsibility (Fig. 1). Local service providers have

978-1-5386-4559-8/18/$31.00 C2018 IEEE

an Information Technology (IT) infrastructure to provide broadband connections.

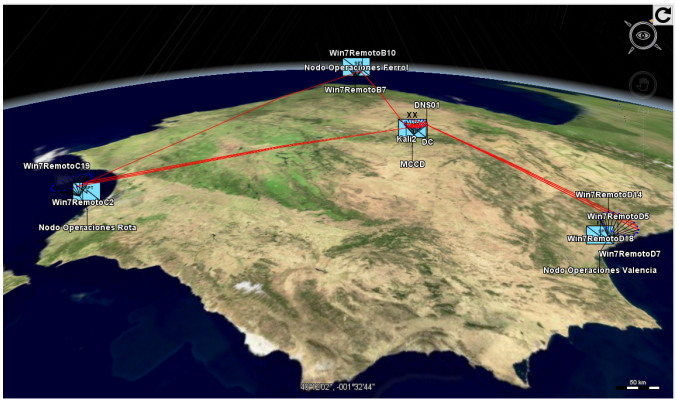

Fig. 1. Simulated cyber-physical environment (from CyCOP system).

"Nodo Madrid" has the main assets of the operation (servers, firewalls, etc.) and the rest of the units are connected with him as a central node. The rest of the nodes are remote nodes.

B. Missions and tasks to be performed.

For the execution of each mission an assessment is made taken into account the capabilities available to perform the tasks by the different units "Nodo Madrid", "Nodo Operaciones Ferrol", "Nodo Operaciones Rota" and "Nodo Operaciones Valencia". These capabilities are considered in terms of associated cyber assets. Existing cyber situation measurement techniques [13] allow a quantitative assessment on cyber impact, mission relevance or risk level

C. Cyber Assets.

The description of the cyber assets related to each node is summarized in Table I.

TABLE I. CYBER ASSETS DESCRIPTION

Unit	**Cyber Assets**		
	C2 & IT	***Communications***	***Remarks***
Nodo Madrid	Division unit Robust, propietary equipment and solutions MOTS	Fiber-optic Ethernet SATCOM	Less subject to be disrupted by GPS jamming
Nodo Operaciones Ferrol	Battalion unit Complex, Interoperable, COTS	SATCOM VHF/UHF Radios	Subject to be disrupted by cyber-attacks
Nodo Operaciones Rota	Battalion unit Interoperable, COTS	SATCOM VHF/UHF Radios	Subject to be disrupted by cyber-attacks
Nodo Operaciones Valencia	Battalion unit Interoperable, COTS	SATCOM VHF/UHF Radios	Subject to be disrupted by cyber-attacks

D. Cyber current situation.

The situation evolves resulting in failures and malfunctioning of fixed information systems. The communications systems installed on vehicles on the move and the authorities' corporate mobile devices are faulty as well. An Advanced Persistent Threat was detected within MINET as part of the accreditation activities conducted by the security authorities.

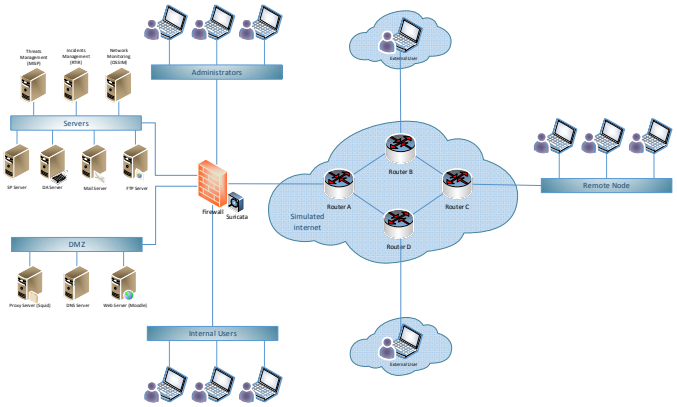

Fig. 2. Scenario network topology.

As shown in Fig. 2, an internal network, which belongs to the division unit ("Nodo Madrid"), is mainly composed of several servers (for Open Source Security Information Management (OSSIM), SharePoint, Mail, FTP, etc.), a DMZ network (for usual services such as proxy, DNS or web server) and both administrator and internal users. A firewall controls the access to the internal network from a simulated internet composed by several routers and both external users and remote nodes (which belong to the battalion units) connected to them.

Communications between assets associated to the "Nodo Madrid" are achieved by fiber-optic or Ethernet, while communications between assets at battalion level are mainly performed through satellite or VHF/UHF radios.

III. COMMON SET OF MEASUREMENTS. SECURITY METRICS

TABLE II.

Proposed Metrics		
Name	***Description***	***Value***
Average Time To Operate (cyber deployable assets)	Average time needed to operate cyber deployable assets under the planned conditions (e.g. individual vehicles or dismounted patrols)	n: the average time to operate deployable assets
Communications Diversity	Number of direct communication links able to establish by different means simultaneously	n: number of direct communication links by different means simultaneously
System Critical Points	A revision of the system architecture can identify critical points subject to be exploited by an attacker	n: number of system critical points

Proposed Metrics		
Name	***Description***	***Value***
Asset Survivability	The survivability aspect of the deployable and fixed network after being degraded, attacked or compromised.	[0,1]: 0 means not operational, 1 means fully operational

IV. 3D OPERATIONAL PICTURE

At the lower tactical or technical levels, a common operational picture is required for decision making within a single domain, for instance a "Common Tactical Air Picture", or a "Cyber Common Operational Picture". At a joint level however, a single "Situation Awareness" needs to be built, that brings together all information from the different domains. For this reason, the "Visualisation for Improved Situation Awareness" (VISA) demonstrator was developed that displays cyber information using conventional military symbols. Since a military commander and his staff are trained to interpret an operational picture expressed using these symbols, they will more easily be able to understand the cyber situation and its impact on the mission as a part of the overarching situation awareness.

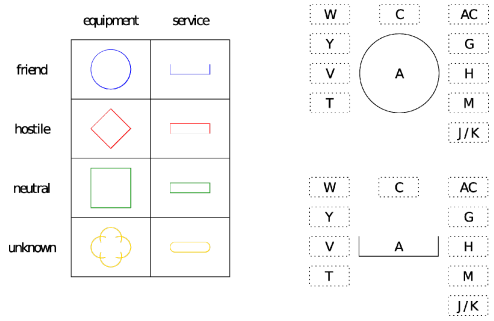

Fig. 3. Main cyber symbols

Figure 3 shows the main symbol types (equipment and service) that are being used in VISA for the different affiliations (friend, hostile, neutral and unknown), as well the conventional locations for adding auxiliary information (such as a Date Time Group (DTG), nation, location, …).

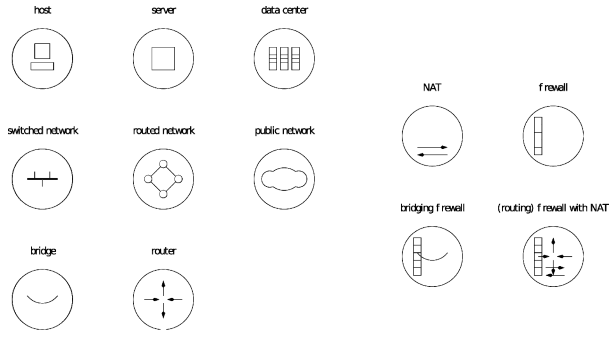

Fig. 4. Equipment types

Figure 4 shows a number of typical equipment types that are represented in VISA, adopting similar design principles as used for the already existing military symbols. The existing concept of capability modifiers was also applied to cyberspace, as is illustrated on the right in the figure.

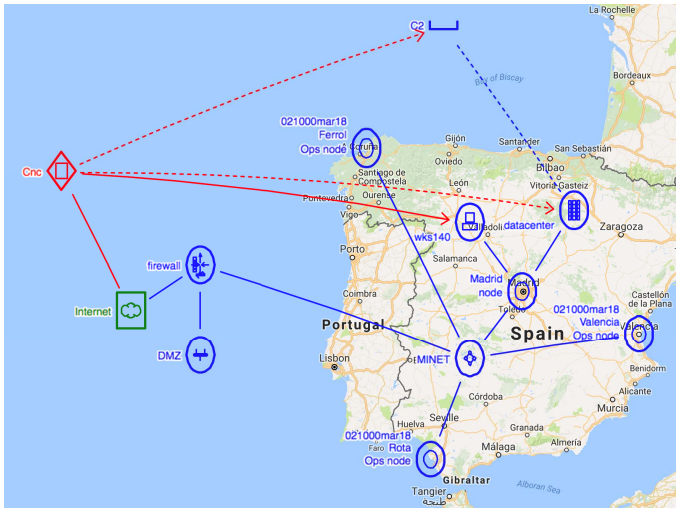

Fig. 5. VISA operational picture

Figure 5 shows the operational picture for the situation described in section II, as it is displayed in VISA at higher level of abstraction. When zooming in, the abstract nodes are replaced by their individual CIS components.

VISA shows the military commander the current cyber situation using a symbolic language he is familiar with. The enemy Advanced Persistent Threat (APT) attack is shown, with the CnC server and the compromised host "wks140". Based on cyber threat intelligence and enemy behavioral modeling, the opponent is expected to perform lateral movement and use the compromised hosts to attack the datacenter and tamper with the command and control service. This is also shown in the VISA operational picture.

The visualisation in figure 5 allows the commander to reach the two first levels of the Endsley model [18]. for situation awareness, being "perception" and "comprehension". What is still missing however, is the third level, which is "projection". For this purpose, a 3D visualisation was developed [1].

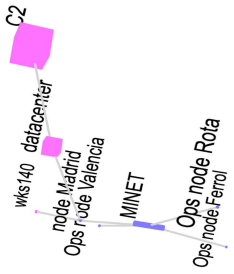

Fig. 6. VISA 3D view of initial situation

Figure 6 shows the current cyber-situation in a 3D view. The user can rotate and pan it using a browser. The size of each node in the graph represents its importance to the mission. Since node of the operational nodes have been assigned a mission yet, it is at this stage primarily the C2 service, offered from the data center, that is important for mission planning. The color ranging from blue to pink shows the importance of the threat, for instance based on cyber threat intelligence or observed attack attempts.

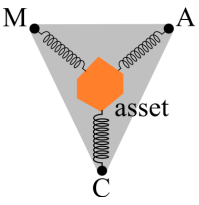

Fig. 7. MAC spring model

The height of a node is determined by a conceptual "spring-model", called the "Mission-Attacker-Controls" (MAC) triangle, shown in figure 7. The forces that pull the node upward are the importance to the mission ("M") and the attacker's interest in the asset ("A"). The force that pulls the object down is determined by the security controls ("C") that are in place to protect the asset. The strength of each force is determined by a fuzzy expert system that implements domain knowledge and applies it to a number of crisp metrics.

The user can inspect a node in the 3D view and display its MAC triangle. He can furthermore do "what if" projections, which is important to explain to the commander the cyber side of the different "courses of action" (CoA's) that are proposed to him by his staff.

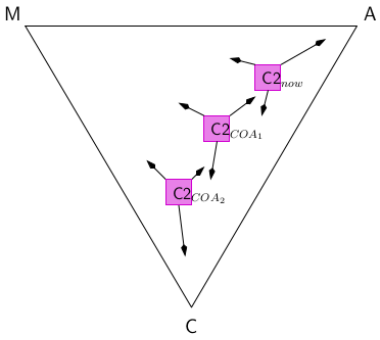

Fig. 8. The MAC triangle for different CoA's

This is illustrated in figure 8, where the current position (labelled "now") for the C2 service is shown in the MAC triangle. The staff officers will propose two possible mitigation CoA's. The first one consists in removing known infected workstations from the network, blocking the known URLs for the CnC channel of the APT and adding appropriate signatures to the Network Intrusion Detection System (NIDS). This mitigation action results in a stronger security control force "C" and a lower threat for the C2 service, and therefore a smaller "A" force. The possibility still exists however that the malware has performed lateral movement and infected a number of other hosts and continues to operate while switching to a new CnC server. Therefore, a second more restrictive CoA consists in additionally implementing a default deny at the network level for all hosts access the C2 system from the Madrid node, except for a limited number of IP addresses that will be explicitly allowed. This tighter security control implementation results in a lower threat and a lower position of the C2 node. The VISA 3D view for COA2 is shown in figure 9.

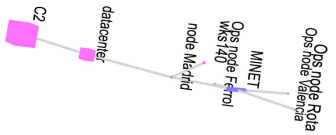

Fig. 9. VISA 3D view for the second CoA

The goal of both the VISA display with conventional symbols on a map as of the 3D view is to help the military commander and the non-cyber members of his staff to better apprehend the cyber situation and assess the cyber aspects of a proposed course of action.

V. CYBER COMMON OPERATIONAL PICTURE (CYCOP)

CyCOP [2] is a C2 information system that feeds on both physical and cyber data, provided by physical systems through NATO Vector Graphics (NVG) protocol [3], and cyber data sources such as Open Source SIEM (OSSIM) [4], Malware Information Sharing Platform (MISP) [5], Request Tracker for Incident Response (RTIR) [6] and risk analysis tools, respectively, merged into a specific data model in order to provide the adequate real-time CyHSA, which can be visualized through the following described advanced representation techniques. Data from cyber sources is obtained, when possible, using cyber security standards for data representation and exchange, as those established and enforced by Structured Threat Information eXpression (STIX) [7] and Security Content Automation Protocol (SCAP) [8].

One of the main features of CyCOP tool is the flexibility to represent any kind of relevant data following the most adequate type of visualization. The representation manager offers a wide set of visualization types summarized in three main categories: 2D/3D charts (bar chart, area chart, pie chart, etc.), dynamic diagrams [9] (hebbian dynamics, bubble chart, force directed graph, etc.) and geo-located representations (generated Keyhole Markup Language (KML) [10], 3D graph and heat map). From the system interface, users can either generate or load, into a data chart container, both customized and predetermined queries after selecting the desired kind of representation.

For instance, Fig. 4 use a hebbian dynamics representation to show the cyber assets (red color) related to each unit (blue color) belonging a specific operation (green color).

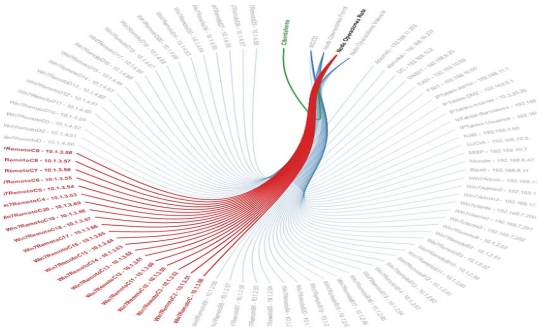

Fig. 10. Cyber assets, unit and operation relationship (hebbian dynamics chart).

In Fig. 5, a circle packing representation shows incidents of each cyber asset grouped together.

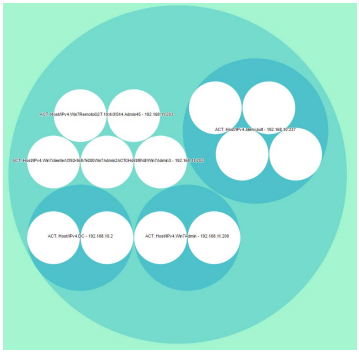

Fig. 11. Cyber asset's incidents (zoomable circle packing chart).

Once again, relationship between cyber assets, units they belong to and current operation is shown in Fig. 6 through, in this case, a code flower representation.

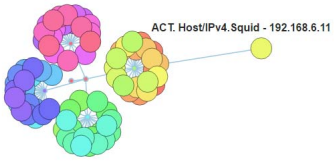

Fig. 12. Cyber assets, unit and operation relationship (code flower chart).

In Fig. 7, combining both georeferenced representation types (generated KML and heat map), cyber asset's incidents of each unit are shown in a geo-located visualization.

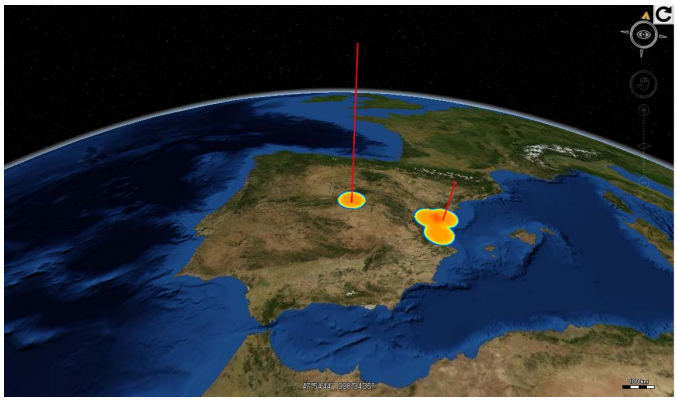

Fig. 13. Georeferenced cyber asset's incidents per unit (generated KML and heat map representations).

In Fig. 8, a 3D graph is shown as the result of a complex generated query representing cyber assets which are georeferenced at the position of the unit they are related to.

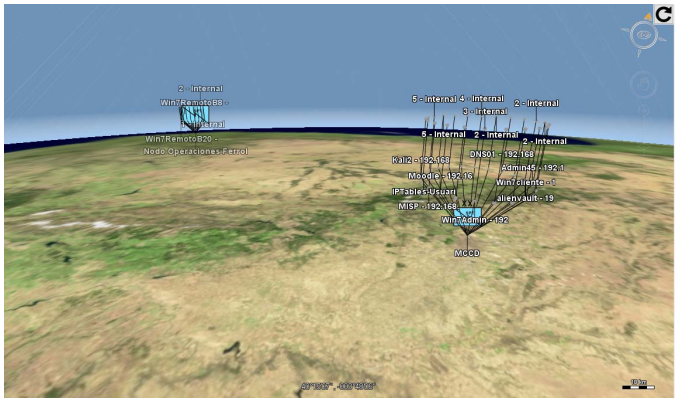

Fig. 14. Georeferenced cyber assets and associated units (3D generated graph).

To guarantee proper CyHSA visualization in a potentially information-overwhelmed situation, when myriads of assets are shown as a result of a given query, CyCOP provides an immersive visualization through the use of Virtual Reality (VR) [11] glasses as an extra advanced representation technique.

Another capability of the system is the threat level functionality. When activated, a gauge range representation, which shows the current threat level of the whole system, is displayed. The threat level is a real-time calculated value following the MAGERIT risk analysis methodology [12].

Finally, the risk analysis tool brings real-time knowledge of the cyber asset's risk level and criticality. To this end, a specific 3D generated graph visualization is shown representing these assets georeferenced to their associated unit's location. In the same way, the consequence analysis tool offers exactly the same information and representation than the risk analysis tool but, in this case, users can estimate the hypothetical system threat level if a specified set of assets is affected by a specified set of incidents. Thus, consequence analysis tool contributes to

decision-making acting as a consequence simulator given a set of incidents as input (Fig. 9).

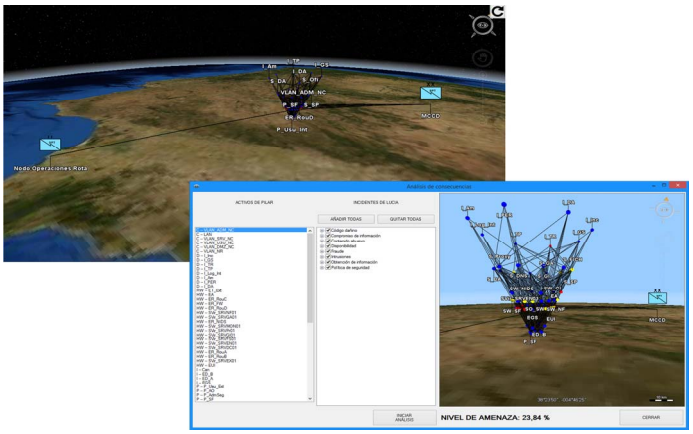

Fig. 15. Risk analysis and consequence analysis functionalities.

VI. COMPARATIVE ANALYSIS

In this section, a qualitative analysis is presented to compare the relevant characteristics of each visualisation technique. The following items express the findings:

a. Both visualisations are complementary. The implementation of external interfaces from CyCOP enables to obtain real-time data e.g. C2 systems, OSSIM and MISP; which in combination with the ability to represent mission criticality aspects from 3D Operational Picture complemented by a risk assessment and mission planning provides a comprehensive cyber situation to a military commander. A vulnerability/threats assessment is imported externally from a service provider or a data source.

b. Different views (representations) contribute to satisfy different user requirements. The tools described in the paper aim to satisfy the visualisation aspects of an operator or technical staff and a decision maker. User-centric solutions drive the engineering implementation of required multi-format representations giving flexibility to operators in their reporting.

c. Real-time data automatically obtained from different sources and sensors contributes to a timely situation awareness representation. Manual data introduction or export from a data repository is a time-consuming effort and generates outdated and non-realistic views. The continuation of a story line is essential in order to evaluate decisions in the past and the progress made when apply remedy actions.

d. CYCOP's granularity, in order to select, filter and combine which information to represent, which visualization technique to choose and where to show data is one of the key features of that system.

e. It is recognised that a major gap exists on the adequacy of comprehensive decision-support systems solutions to achieve an enhanced cyber situation awareness. The ultimate goal of a visualisation is to assist military decision makers and technical staff in their comprehension of the cyberspace.

f. Mission oriented. The association of cyber assets to nodes ("Cyber ORBAT") is the approach adopted to assess the level of criticality for a mission. In that sense, a military planner introduces the relationships between cyber assets employed and the type of mission. As a result, the representation should be intuitive and permit to identify risks at a first glance.

VII. CONCLUSIONS AND FUTURE WORK

The authors deem necessary to conduct an experimental validation with operators-administrators working in a military Computer Emergency Response Center (mil-CERT) or in a cyber incident handling cell to test if the proposed visualisation techniques are fulfilling their needs in daily operations. This experimental validation may use the Situation Awareness Global Assessment Technique (SAGAT) [14] as a methodology originally developed to assist pilot-vehicle interface designs by providing an objective measure of pilot´s situation awareness. In that respect, a variation of the target audience (operators-administrators and military decision makers) and the operational domain cyberspace will modify some of the characteristics validated in the methodology proposed by SAGAT. Other possible improvement to approach visualisation techniques for cyber situation awareness is related to the information classification and decision-making. Extensive research is being made to design artificial intelligence algorithms in an unsupervised [15] [16] way to let the machines learn sufficiently from the experience. Automatic refinement of visualization [17] is envisaged as a promising technology facilitated by artificial intelligence where data is processed and classified accordingly depending on the risk levels. That possibility may improve the efficiency on incident handling and save time for decision making.

REFERENCES

[1] Wim Mees, Salvador Llopis, Thibault Debatty, "Achieving cyber situation awareness through a multi-aspect 3D operational picture" NATO IST-148 Symposium on Cyber Defence Situational Awareness, October 2016.

[2] Manuel Esteve, Israel Pérez, Carlos Palau, Federico Carvajal, Javier Hingant, D. Comunicaciones, Universitat Politècnica de València; Miguel A. Fresneda, Juan P. Sierra, Spanish Joint Cyber Command, "Cyber common Operational Picture: A tool for Cyber Hybrid Situational awareness improvement" NATO IST-148 Symposium on Cyber Defence Situational Awareness, October 2016.

[3] NATO Standard ADatP-4733, "NATO Vector Graphics Specification", Edition A Version 1, NATO Standarization Organization (NSO), April 2017.

[4] OSSIM, https://www.alienvault.com/products/ossim

[5] MISP, http://www.misp-project.org/

[6] RTIR, https://bestpractical.com/rtir/

[7] STIX, https://stix.mitre.org

[8] SCAP, http://scap.nist.gov/

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

[10] KML, https://developers.google.com/kml/documentation/kmlreference?hl=en

[11] D. Chu, "Toward Immersive Mobile Virtual Reality", Proceedings of the 3rd ACM Workshop on Hot Topics in Wireless (HotWireless '16), isbn: 978-1-4503-4251-3, New York, 2016.

[12] "MAGERIT – version 3.0, Methodology for Information Systems Risk Analysis and Management", Spanish Ministry of Public administrations, Madrid 2014.

[13] Tadda, G.; Salerno, J.; Boulware, D.; Hinman, M. & Gorton, S. (2006). Realizing Situation Awareness within a Cyber Environment, In: Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006, edited by B. V. Dasarathy, Proc. of SPIE Vol. 6242, SPIE, Bellingham, WA, 2006.

[14] Endsley M. R. (1988), Situational awareness global assessment technique (SAGAT). Proceedings of the National Aerospace and Electronics Conference. 789-795.

[15] MacQueen, J. B. (1967). "Some Methods for classification and Analysis of Multivariate Observations". Proceedings of 5th Berkeley Symposium on Mathematical Statistics and Probability 1. University of California Press. pp. 281–297.

[16] B. Schölkopf et al., "Nonlinear component analysis as a kernel eigenvalue problema", Neural Computation, Volume 10 Issue 5, July 1, 1998, Pages 1299 – 1319, MIT Press.

[17] Enrico Bertini and Denis Lalanne, "Investigating and reflecting on the integration of automatic data analysis and visualization in knowledge discovery", SIGKDD Explor. Newsl. 11, 2 (May 2010), 9-18.

[18] Endsley, Mica. (1995). Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64. Human Factors: The Journal of the Human Factors and Ergonomics Society. 37. 32-64. 10.1518/001872095779049543.