Cyber Situation Awareness

Dr. Margaret Varga
Seetru Ltd., Albion Dockside Works, Bristol, BS1 6UT, UNITED KINGDOM
and
University of Oxford, South Parks Road, Oxford, OX1 3SY,
UNITED KINGDOM
Email: margaret.varga@seetru.com / margaret.varga@zoo.ox.ac.uk

Dr. Carsten Winkelholz and Susan Träber-Burdin
FKIE, Fraunhoferstrasse 20, 53343 Wachtberg,
GERMANY
Email: carsten.winkelholz@fkie.fraunhofer.de and susan.traeber@fkie.fraunhofer.de

ABSTRACT

"A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11" Leon E. Panetta, US Secretary of Defense, October 2012.

This paper discusses the application of User Centered and System Based approaches to cyber situation awareness.

1.0 INTRODUCTION

We are increasingly dependent on the ever expanding Internet with its growing complexities and inter-dependencies. While on the one hand its immensely powerful infra-structure underpins society, on the other hand its vulnerabilities to cyber-attack pose huge risks to society and national security. Cyber attackers can cause widespread network destruction remotely, anonymously and at low cost. The attacks can be conducted through denial-of-service (DoS) or distributed denial-of-service (DDoS) etc. [13 and 25].

In Spring 2007 the DDoS attack in Estonia targeted government websites as well as websites of banks, universities, and Estonian newspapers. The Estonian government decided to stop all international web traffic, thus cutting off the entire country from the rest of the world. After three weeks the attacks stopped abruptly. This is a vivid illustration of why cyber defence is a growing concern for safe-guarding national security. In 2008, NATO set up the NATO Co-operative Cyber Defence Centre of Excellence in Tallinn.

NATO 2020 states - *Responding to the rising danger of cyber-attacks: NATO must "accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence."* [23].

Cyber situation awareness is vital in support of making informed decisions for maintaining a safe and secure environment [6, 8, 14 and 19]. The enhancement of the cyber operators' situation awareness is thus the goal for any interface design.

2.0 CYBER SITUATION AWARENESS

What is situation awareness? In the simplest term, it means being aware of ones surroundings. A search of 'definition of situation awareness' on Google returned 596,000 links. However, Endsley's work on situation awareness (SA) is an established definition of SA, in particular for dynamic environments:

"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future." [10].

Endsley considered that there are three stages of situation awareness, namely: (1) perception, (2) comprehension and (3) projection [10]. This links cognitive psychology with human factors in the explanation of making sense in complex situations, such as the cyber domain.

In cyber defence operations all three stages are continual round the clock functions, because they are tightly interlinked. Awareness includes awareness of network services availability, confidentiality, operations and integrity, etc. It also encompasses decisions on configuration and policy, scanning mechanisms, strategy on monitoring, detection and responses. It thus requires awareness of the network infrastructure and the security aspects of both the physical and cyber domains. Effective cyber situation awareness, and thence cyber security management, must not only be reactive but pro-active, and thus be able to make predictions as to the state(s) of the situation. In order to support the users in their operations and the awareness of the cyber situation the analysts need to be able to detect, recognise, identify and communicate trends, patterns and anomalies in a timely manner [9 and 20].

To be effective security analysts must thus:

- have a constant and clear understanding of the status, health and performance of the networks;
- be able to detect, recognise and identify any patterns or trends;
- be able to detect, recognise and identify any changes or anomalies, and recognise their significance in a timely manner;
- be able to communicate, present and update the situation clearly and succinctly.

The challenges faced by the analysts are:

- How to manage, process, filter and analyse the massive amount of data from different data sources regarding the network activity, i.e. complex, diverse and noisy data.
- How to manage the dynamic network topology.
- How to understand the operation and the status of network system:
    - What is the purpose of the system?
    - What is the network infrastructure?
    - Where and what are the vulnerabilities?
    - What are the network components?
    - What are the relationship and interrelationship in the network?
    - What are the dependencies?
    - What type of effect or impact? Sequential / consequential / isolated?

The main challenge is how to present the massive volume of dynamic and complex data in a tractable, comprehensible and usable manner that enables the analysts to make sense of the data thus maintain effective

cyber situation awareness [21, 22, 32, 39 and 41].

It is often said that a picture is worth a thousand words; in the case of cyber operations a picture is worth millions of log files. The use of visual aids is a well-established practice, they are used by humans as essential tools to help them define, understand, analyse, explore, explain and navigate their way through their tasks / problems to understand the situation and so enable informed decision making

In short, cyber situation awareness encompasses the human cognitive process and the processing of data. In the complex and dynamic cyber environment, acute situation awareness greatly enhances the rate and the quality of human decision making. This paper will discuss different human machine interface design approaches applicable to addressing presentation and analysis for cyber situation awareness.

3.0 CYBER SITUATION AWARENESS AND VISUAL ANALYTICS

There are different tasks in cyber security and D'Amico [7] developed a nine-way taxonomy:

1. Triage analysis: Weed out false positives, escalate suspicious activity for further analysis.
2. Escalation analysis: Analyze data over longer time and incorporate multiple data sources.
3. Correlation analysis: Look for patterns and trends and assess similarity to related internal and external incidents.
4. Incidence response: Recommend, implement Courses of Action and support law enforcement investigation.
5. Malware analysis: Reverse-engineer malware and develop defences against malware.
6. Forensic analysis: Collect and preserve evidence and support law enforcement investigation.
7. Threat analysis: Characterize attackers, their identification, modus operandi, motivation and location.
8. Vulnerability analysis: Identify and prioritize vulnerabilities to manage remediation of vulnerabilities.
9. Sensor management: Develop signatures, tune sensors and modify placement of sensors.

Figure 1 shows the relationship between the above first eight tasks in the three stages of situation awareness and visualization [7]; it can be seen that the three stages are inter-linked.

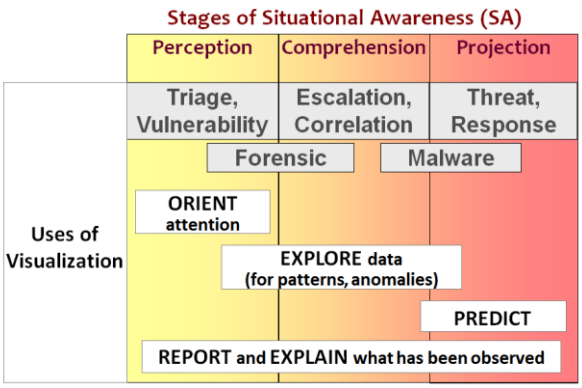

Figure 1: Relationship between the stages of situational awareness, the use of visualization and the types of analysis performed [7].

The roles of visualization and visual analytics are essential in maintaining situation awareness. The need to explore data for patterns and anomalies as well as reporting and explaining what has been observed cut across all three stages. Triage, vulnerability and forensic analysis enable attention orientation to be conducted during the perception stage, while escalation and correlation analysis are conducted during the

comprehension stage. Forensic analysis is conducted not only during the perception stage but the comprehension stage as well, while the malware analysis is conducted during the comprehension and projection stages. This shows how visualization / visual analytics are used to support the analysts to assess the situation and thus make informed decisions, for instance, to manage the detected threats, i.e. how best to contain; isolate; minimise, mitigate, recover from the attacks. The three stages of situation awareness (perception, comprehension and projection) are tightly integrated, and visualization and visual analytics provide the necessary means to support the three stages.

Visual Analytics is the science of analytical reasoning facilitated by interactive visual interfaces [35]. It exploits interactive analysis, visualization and human cognitive abilities to provide an extremely powerful methodology to support situation awareness and decision making. It can provide an effective means for analysts to see, interact with, explore and compare data of different dimensions at multiple granularities and in real-time, i.e. to undertake sense making, and this allow for the detection of trends, patterns, changes, anomalies and weak points [15, 17, 26, 36 and 44].

4.0 HUMAN MACHINE INTERFACE DESIGN APPROACHES

Different approaches to human machine interface design can be developed and applied to address the different operational and users' needs, for example:

- user centered approaches [11, 18, 24, 35, 37 and 38] on one hand, and
- system based approaches, such as the Ecological Interface Design (EID), on the other hand.

These two approaches are radically different in their manner of providing situation awareness.

The user centered approach focusses on the users' and tasks' needs, the users' skills and limitations as well as their mental models [2 and 43]. Whereas an EID is an interface design specifically suitable for real-time dynamic and complex socio-technical systems [40]. It is a methodology to communicate complex work domains in a cognitively effective manner through different abstraction levels [30]. An EID interface design focuses on the system, work environment or work domain [27, 28 and 29]. An EID is composed of two concepts: firstly, the Abstraction Hierarchy (AH) to model the work environment; and secondly, the Skills, Rules, Knowledge (SRK) framework to define how the information should be visualized [31]. The aim is to make constraints and complex relationships in the system / work environment intuitively clear to the user in an informative manner.

5.0 USER CENTERED VISUAL ANALYTICS

The user centered approach is determined by, or structured according to, the user's needs and tasks, with the support of the necessary data. The provision of the necessary tools requires in depth understanding of the users, their needs, how they work, what are their tasks, what sort of data they need to do their tasks, the users' skills and limitations as well as their mental models [2]. In this case intuitiveness and fluidity is an important factor in supporting the users [43].

Visual Analytics exploits interactive visualization and human cognitive abilities [17, 33, 34 and 35]. It enables the user to explore and analyze data from different sources through integrated interactive visualizations. Visual Analytics offers a powerful data driven methodology applied in a user centered manner (user centered visual analytics): it focuses on the users and operates at a rate that is resonant with the speed of human thought [15 and 43].

In the Cyber domain vast volumes of different types of data from different sensors are generated by the second every day. This presents a huge challenge to maintaining situation awareness [12]. Much active

research in the field has been conducted into developing and applying visual analytics techniques to make sense of the dynamic and complex data with the aim of providing cyber situation awareness. These approaches have been data driven for two reasons:

- Log-file data is the data that is readily available.
- Administrator's tasks are typically to search in log-files for specific entries in order to make sense of malfunctions in the network or alerts from IDS-systems.

To facilitate these tasks it is common to write the log-file entries into a database. This enables fast search queries on this vast amount of data and facilitates the production of statistics on, for instance, frequencies. It is necessary to integrate these often complex, voluminous and dynamic data / information in ways that fit the different goals, tasks and needs of the users. The integration plays a significant role in making the different types of information available in an accessible representation; c.f. relying on users' mental correlation, which is time consuming and can quickly exceed the human's information processing capabilities - leading to errors in decision making: Users face information overload, leading to poor situation awareness [11].

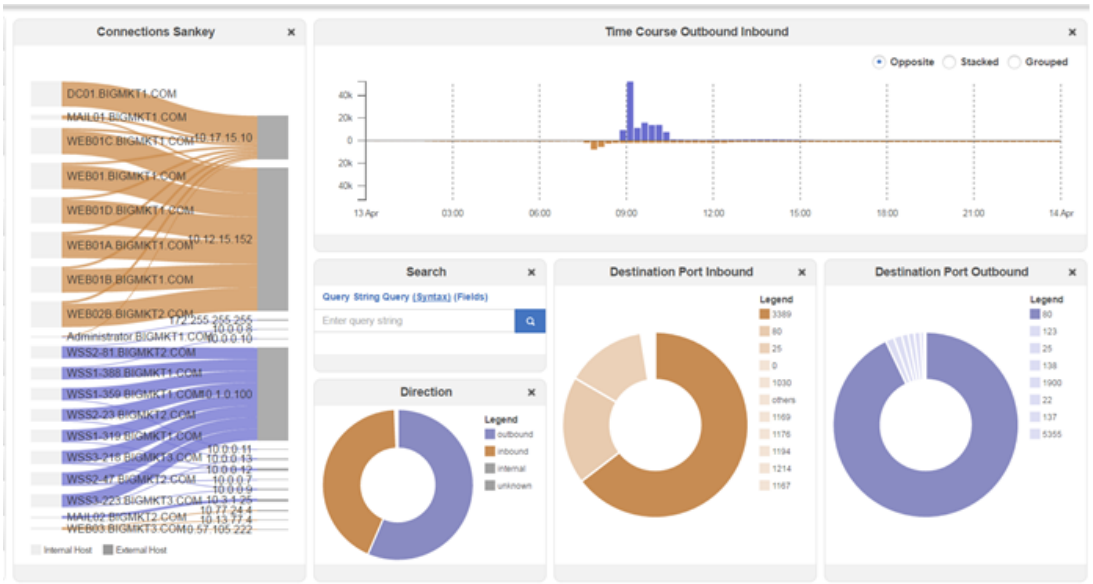

Figure 2: Netflow analysis

Using the example data from the IEEE VAST Mini Challenge 3 [16] Figure 2 shows a DDoS attack from eight infected own hosts, within the Big Marketing Corporation network, on an external server (10.1.0.100). The Sankey diagram on the left hand side is used to show the inbound (brown) and outbound (blue) traffic [41]. Furthermore, the Sankey shows scanning activities from two external hosts.

The bi-directional bar chart shows the outbound and inbound traffic in the opposite directions. The donut rings show the inbound and outbound traffic together and separately and their associated ports.

The above shows netflow statistics through different visualizations such as line charts, bar charts, pie chart (donut ring), Sankey etc. Additionally these visualizations can be used to filter on the data by just selecting attribute values from any of the displays in the dashboard, the corresponding features in other displays will be filtered and visualized accordingly. The analyst can also drill down into the data, i.e. details on demand. This intuitive approach for exploring big data has become available because of the progress in database technologies which enables filtering, analysing and calculating aggregations on billions of documents in near real time [5].

6.0 ECOLOGICAL INTERFACE DESIGN

The previous section considered the user centered visual analytics approach, an approach which focuses on the user. Ecological Interface Design (EID), on the other hand, focuses on the system, work environment or work domain [40]. It is based on the idea that by understanding how a system works, people can manage and diagnose problems in a system more effectively and efficiently. The knowledge of the system can thus be used to build a display interface that helps the users understand the system that they are managing and monitoring. In this manner, an EID enables the user to navigate through the system and solve problems in familiar or similar situations as well as in unexpected situations. This approach has been applied to complex systems such as military command and control, aviation, process control and medicine, and recently to computer network defence [1, 3 and 4].

EID is based on work domain analysis and is composed of two concepts, namely the Abstraction Hierarchy (AH) and the Skills, Rules, Knowledge (SRK) framework [30, 31 and 40].

Table 1 shows the Abstraction Hierarchy that uses a 5-level functional decomposition to model the work environment or the work domain [27 and 30], i.e. how the system works. It shows that in the EID framework the AH is used to determine what sort of information should be shown on the system interface and how the information should be organised. Each level describes the same system at different levels. At the top-most level the Functional Purpose defines the purpose of the system, i.e. what it does. While in the second level the Abstraction Function is concerned with the causal structure of the process, such as information flow. The general work activities and function of the system are defined in Generalized function at the third level, whereas the physical capabilities and connectivity between them are defined in the fourth level - the Physical Function. The Physical Form at the bottom level is concerned with the appearance, location as well as the configuration within the overall structure of the system.

Table 1: Abstraction Hierarchy

Functional Purpose	Purpose for which system was designed
Abstraction Function	Intended structure of the process in terms of mass, energy, information or value flows
Generalized Function	General work activities and functions of the system
Physical Function	Physical processes components and connections between them
Physical Form	Appearance. Location, and configuration of component

The benefit in representing domain information in a work domain model is to enable the operators to develop an in depth understanding of their system or work environment by analysing the different variables across the various different levels. The hierarchical structure shows the ‘how’ (top-down) and the ‘why’ (bottom-up) relationship in the design. This information can then be used to identify information that need to be addressed in the interface.

The Skills, Rules and Knowledge framework (SRK) defines three types of behaviour and was developed to support the combination of information requirements for a system and the human cognition, i.e. how information should be visualised [31]. The decision ladder shows a template for mapping an operator’s cognitive processes on a set of information processing activities and cognitive (knowledge) states, see Figure 3. There are 3 stages to applying the SRK framework, namely: situation assessment, option analysis &

planning, and execution of action. In Figure 3 the rectangles represent information processing activities while the ovals represent the states of knowledge from the information processing activities. The left hand side of the ladder is concerned with activation, observation and identification so as to enable awareness of the current situation, such as where are we now, what is happening and what is the consequence? Moving up the ladder involves judgement, prioritization, and selection of alternatives. The right hand side of the ladder consists of elements to enable planning and carrying out the tasks using the available resources – so as to change the current situation when necessary. The situation could be normal, routine, planned, unique, unexpected or high risk. The SRK Framework supports skill-based and rule-based behaviour for familiar / routine tasks, and thus enables the user to devote more cognitive resources to knowledge-based reasoning for detection of unexpected events or anomalies, solving problems and making decisions

6.1 Application of EID in Cyber Defence

In the military / defence situation, however, the operational requirements are prioritised. The system designer cannot consider all possible operational requirements, which might be very dynamic with a large number of variations. The system designer therefore has to focus on a subset of prioritised operational requirements. Figure 4 illustrates, using the decision ladder, the trade-off that the operator / commander might have to decide upon in respect of availability and security.

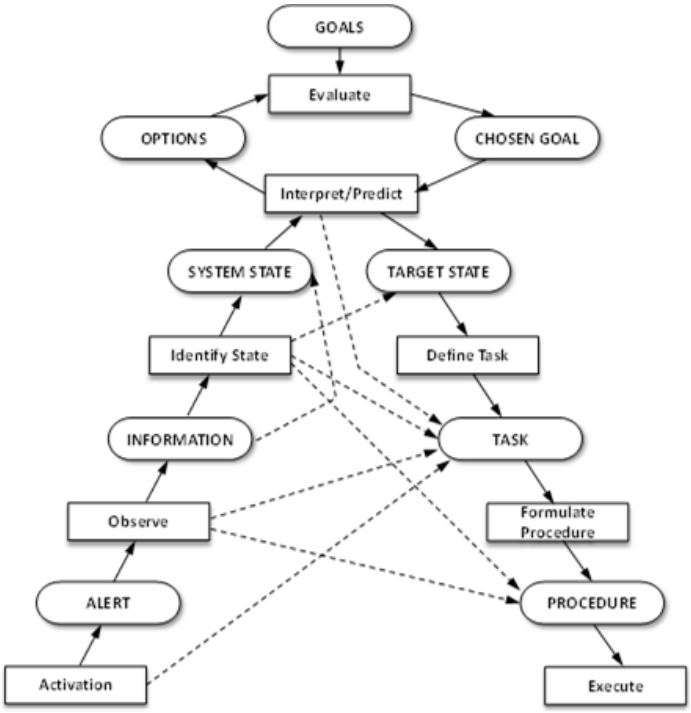

Figure 3: SRK Framework - Decision ladder adapted from [31]

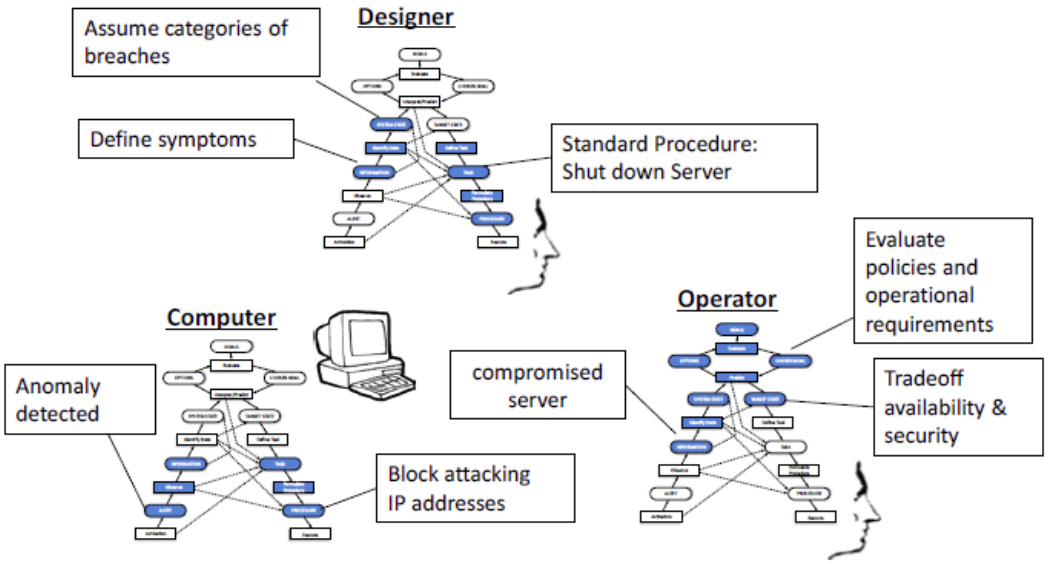

Figure 4: Decision Allocation where the operator set the goal priorities [42]

The visualization required differs at different levels, see LHS of Figure 5. The possible transition points in the decision ladder correspond to specific abstraction levels used in the work domain analysis, see Figure 3 and Table 1. The decision on the desirable target states of the system corresponds to the functional purpose level of the abstraction hierarchy. The alert level on the other hand adheres to the data level and physical level. On the upper levels, visualization should support the understanding of the systems and its constraints, while on the lower levels visualization should support the analysis and the understanding of the system's components and raw data. The stages of information processing from the SRK-model can be used to categorize user interfaces and Automation / Artificial Intelligence in Cyber Defence: see Figure 5 which shows how both the SRK and AH Framework can be used to categorize tools and functions of Cyber Defence systems. The SRK Framework focuses on the tools of automation and algorithms (RHS) while the AH Framework focuses on interfaces to the human operator (LHS). At the low level, raw data can be analysed by detecting anomalous pattern that triggers alerts: raw data could be network data captured at the network interfaces. The raw data can also be presented to human operators to exploit the human ability to detect patterns. At the upper level, more context information is used to process the data. On this level human operators need an operational picture that allows them to take the physical constraints of the network into account [29].

In order to keep the human in the loop effectively it is necessary to make the information from the abstract data accessible to the analysts in an intuitive manner that fully exploits his perceptual senses and supports his mental models - so he can understand the displayed information and thus the situation. There are two possible modes, namely, a goal-oriented mode, and an exploration-oriented mode. In the goal-oriented mode, an analyst tries to track down root causes of specific events whenever he senses any anomalous behaviour, while in the 'exploration' oriented mode the adaptive nature of human information processing is utilized to detect and identify unusual behaviour and events within the network. Humans are good at learning / remembering patterns that characterise normal behaviour and are equally good at noticing changes. However, this is more to do with sensing common patterns of environmental factors and is not necessarily related to logical reasoning. Within the 'exploration' mode the user observes patterns through visual displays that represent a system state. Thus, in the exploratory mode it is important to cover a broad spectrum of the data within the visualization, following the principle "above all else show the data" [36]. Therefore, both modes need to be consistent in their representation so as to allow the analyst to switch easily between the two modes.

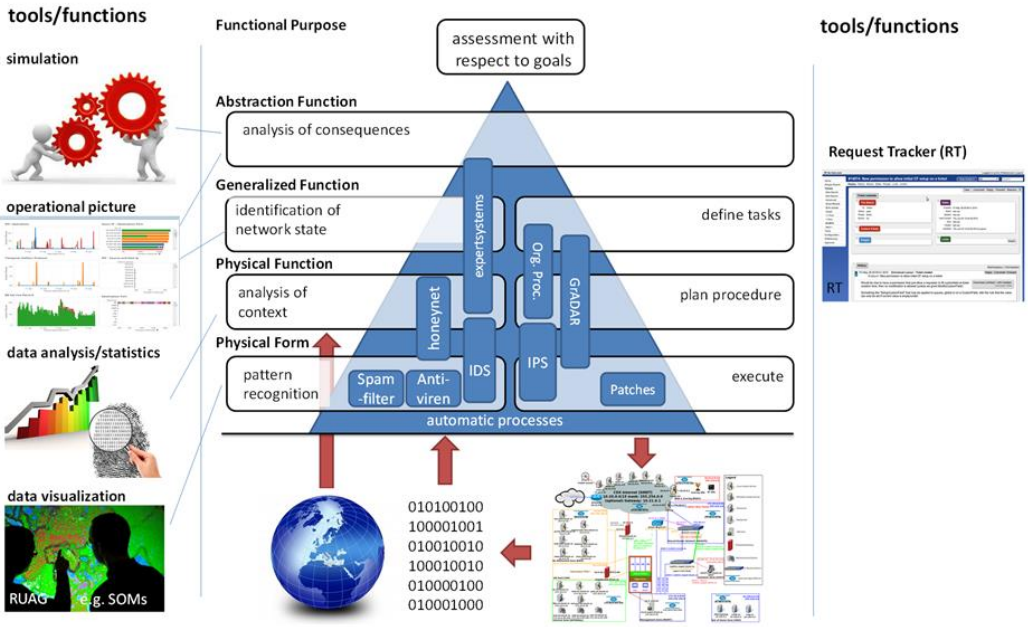

Figure 5: Categorisation of User interfaces and Automation/Artificial Intelligence in Cyber Defence [42]

6.2 Application of EID to Network Management

Burns *et al.* [3 and 4] developed a work domain model for monitoring network performance and availability. They applied the analysis of the network management to the Application, Network, Data and Physical layer of the OSI model. For simplicity they grouped the Transport, Session and Presentation layers into the 'Application' layer, to reflect the end-user communication, see Figure 7. Figure 6 shows the mapping of the Abstraction Hierarchy into the first four layers of the OSI model [3 and 39].

	Application	Network	Data Link	Physical
Functional Purpose	• Share information communication • Assure availability of Network services	Maximize Availability	Minimize errors	
Abstraction Function	**IPC:** • clients • servers • middleware	**Internet traffic:** • Data sources • Data sinks • Data transfer between networks	**LAN traffic:** • Data sources • Data sinks • Data transfer between devices	**Signal transmission:** • Signal sources • Signal sinks • Signal transmission in physical medium
Generalized Function		• Traffic routing and prioritization • Broadcast containment	• Network segmentation • Error checking • Packet switching and retransmission	• Signal generation and propagation • Collision detection
Physical Function		• routers	• Switches • Bridges • Hosts	• Network interface • Cable
Physical Form		• Network topology	• Physical spec of devices • Plocation of device	Cable form (e.g. Twisted pair, coaxial)

Figure 6: OSI Model and Abstraction Hierarchy

The approach focuses on information from the data sources to data sinks, at different level of detail, from data transfer between networks, data transfer in local area networks (LANs) and data transfer across the physical medium. Burns *et al.* [3] set the top level as the functional purpose of the system to maximise the throughput of communication between distributed applications, which they further decomposed into sub-goals of maximising availability and accuracy, and minimising delay.

At each abstraction level different information is required; for example, at the top level overall performance features should be displayed in the functional purpose network. The operator needs to understand the cause / reason whenever the performance network is above or below a certain predefined threshold. For example, at the abstraction level view, the information flow is needed in order to identify the possible problems / bottlenecks. Furthermore, if there are suspicious activities the operator needs to inspect the states of the network equipment as well as the parameters in the configuration.

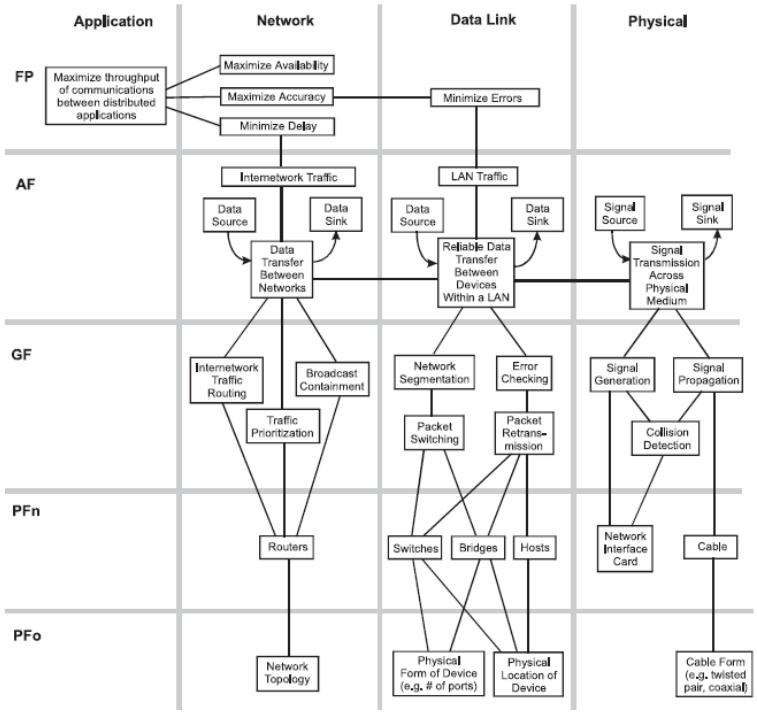

Figure 7: Work domain representation of the network performance management [3]

Figure 8 shows an overview of the functional purpose display of the topological layout of all the switches and routers in a network [3]. Each device is colour coded using a traffic light colour scheme, namely green for normal, yellow for warning and red for critical. The LHS of the display shows a relatively healthy network while the RHS shows problems in the network. The height of the stacked bar chart represents the number of devices that are in the warning, critical or down states. In this display the network operator can easily see where there the problems are and their extent, i.e. the higher the bar the less healthy is the network. This is also used for navigational purposes within the main view (Figure 9), i.e. clicking on a point will result in showing the corresponding areas of the network in the main view.

Figure 9 shows the 3-dimensional logical view of the network, where switches that are logically assigned to one VLAN are placed together in a circle. Furthermore, each area is linked to every other area to represent the logical connections between them. In addition, logical links are displayed between each switch and every other switch with the same VLAN to represent the degree of intra-LAN communication.

The links are colour coded to represent the link activities. Dull green is used when the traffic is light and the utilization level is low. Yellow is used when the traffic exceeds a warning threshold and red when it is nearly saturated with high volumes of traffic that cause network congestion and delays in transmission. The display thus provides the network manager with an overview of the utilization of links within and between different VLANs. Figure 9 shows a single red line between VLAN 33 and 39 which is represented as a red square in the matrix. All other inter-VLAN links are operating normal so they are in green. The inbound and outbound are represented by the two halves of the matrix along the diagonal line. The column represents the VLAN from which the traffic comes and the rows represent to where the traffic is directed. This provides directional information between all the VLANs. Other additional displays such as the polar star is used to show information of the Generalized Function level such as broadcasts, multicasts, errors, packets, octets and utilization. They are displayed above the main display.

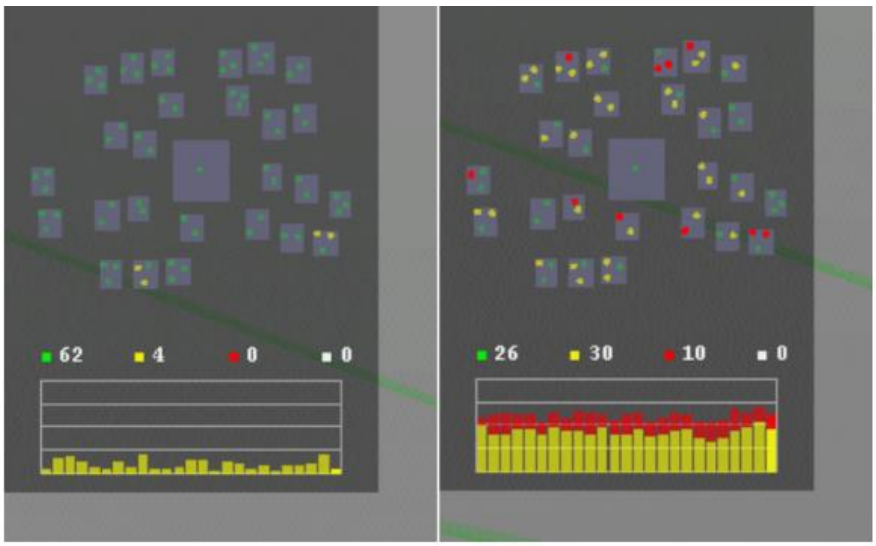

Figure 8: Functional Purpose Display. LHS is a relatively healthy network while the RHS shows a less healthy network [3]

The performance of the tool was evaluated against the Hewlett-Packard OpenView Network Node Manager (NNM). It showed that the EID tool was more effective and accurate in diagnosis than NNM, though detection took longer. This illustrates the effectiveness of the EID approach in network management; the authors, however, acknowledged the challenge of scalability and complexity as well as the application to VPNs.

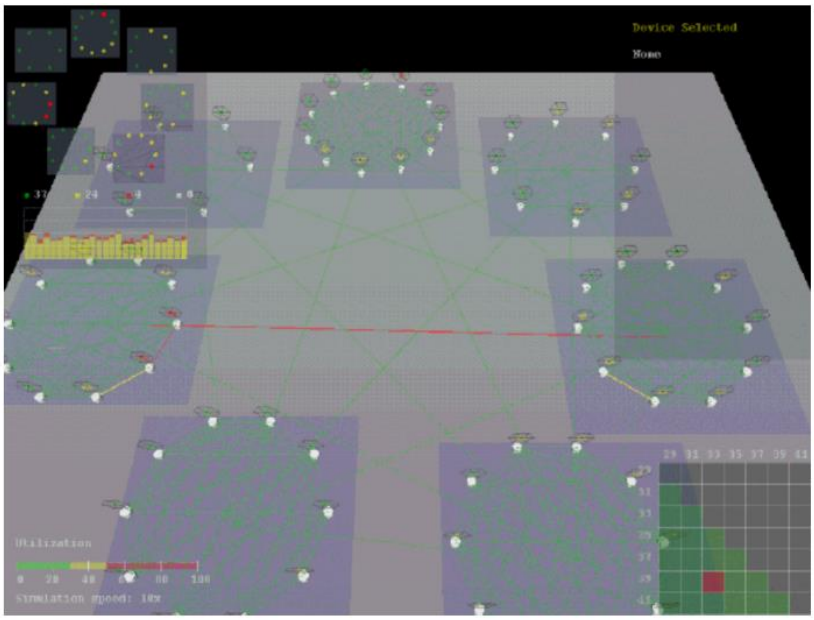

Figure 9: 3-dimensional Logical view of residence network in Visual Network, showing traffic levels between and within different VLANs [3]

6.3 Application of EID for Computer Network Defence – VEILS

VEILS (Versatile Ecological Interface for Lockdown network Security) is a prototype system developed for Computer Network Defense (CND). It uses the Ecological Interface Design (EID) framework. It integrates multiple data sources such as IDS, IPS, firewall, and system logs. Its design principle are based on direct perception, direct manipulation and visual momentum [1].

Figure 10 shows the six different displays in VEILS. In the network overview, it uses icons to display the network components such as routers, web server, an IDS etc. - a network physical view.

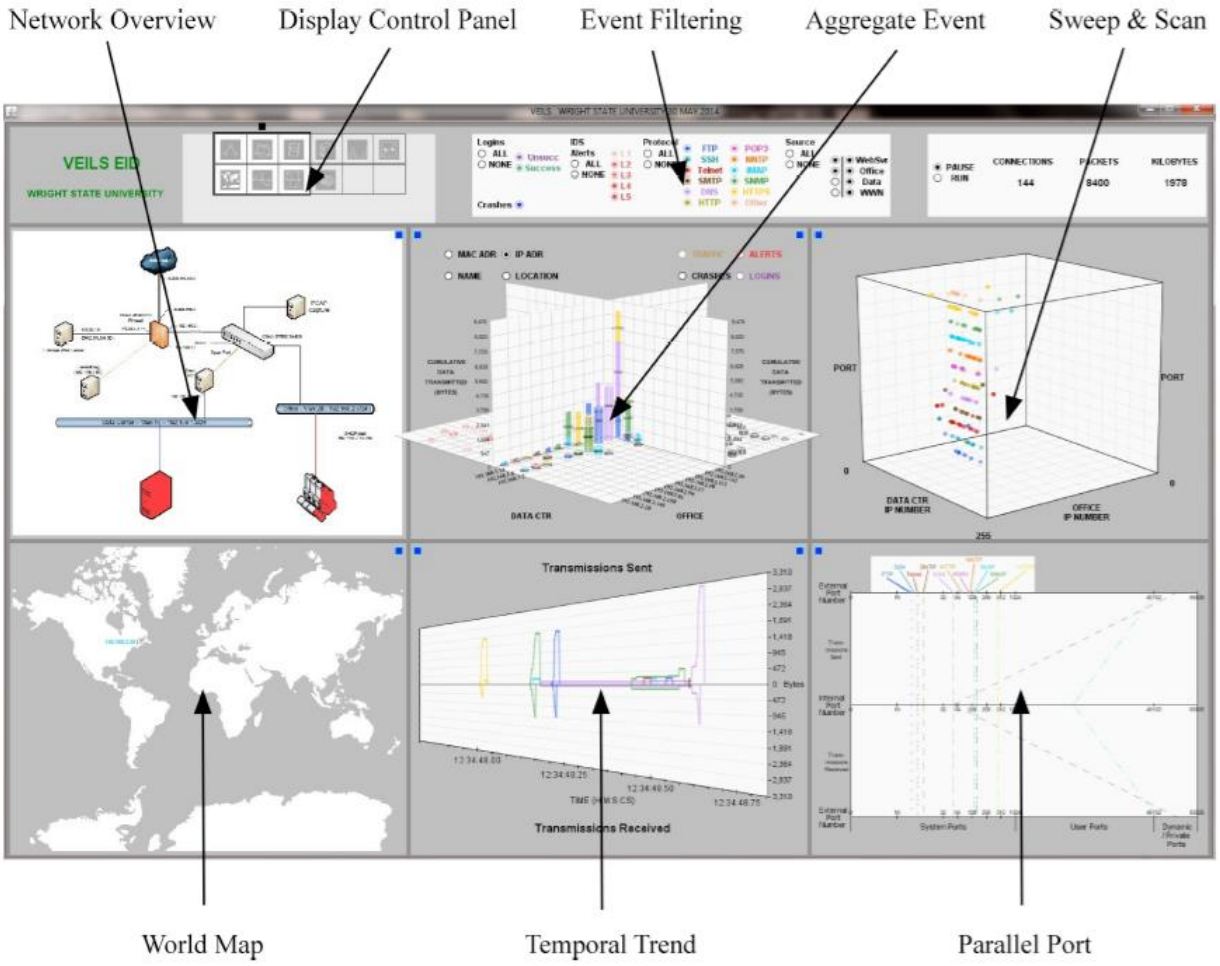

Figure 10: VEILS [1]

The aggregate event display is a 3-dimensional cube that provides an overview of the system events, i.e. IDS alerts, protocols and the reasons for the events in question. The matrix at the base of the cube represents machines of different categories and each cell in the matric is the interaction between the two corresponding machines. The height of the 3-dimensional columns graph corresponds to the total amount of data transmitted between the machines. Furthermore, the overall amount of data transmissions by an individual machine is represented by the three dimensional bar graph at the back of the cube. The protocols are colour coded. The Temporal Trend Display shows the temporal patterns of system events, such as protocols, crashes etc. The outbound and inbound traffic are represented on the upper and lower portions respectively. The direction, rate, time period and size of transmission are represented by different trend line and colour coded by data protocols. The computer ports and data protocols and their compatibility with the network security plans are displayed in the Parallel Port Display. Three axes are used to represent the external source port (upper axis), internal network port number (middle axis) and the destination port of the internal network (lower axis). A vertical line indicates that the same ports origin and destination was used for transmission, c.f. non vertical lines use different ports. Colour and dash patterns are used to represent alternative data protocols. Three ranges of ports are displayed according to their properties, namely 0-1023 are system ports, 1024-49151 are registered ports while 49152 – 65535 are dynamic and/or private ports. Their properties governed the scaling scheme employed to provide visual clarity, such as linear scale, logarithmic scale and binning. The Sweep & Scan displays an overview of the scanning activities. The x-axis represents IP addresses of a set of computers that are being protected while the y-axis represents their associated ports. The z-axis shows the monitored IP addresses for their scanning attempts, their failed attempts are represented

as colour coded dots.

The user can have an overview of the network activities and drill down to problems of concerns. VEILS provides an effective EID for cyber defence by providing the overview of the system performance and details information such as scanning, in-bound and out-bound traffic, etc.

7 CONCLUSIONS

Two different human machine interface design approaches for cyber situation awareness were discussed, namely, the user-centered approach and the system based Ecological Interface Design (EID) approach. The two approaches are radically different in the manner in which they provide situation awareness; they are, however, complementary to each other. To find valid explanations of an event in question the analyst needs a deep understanding of the physical and logical constraints of the network system and the EID reflects these constraints. Whereas user centered visual analytics is more appropriate for the case of the analytic process and display of dynamic data with detailed information on the performance of network components, such as IPs, ports, protocol, packages, CPU load, disk and memory usages, etc.

.

8 REFERENCES

[1] Bennett, K. B., VEILS: An Ecological Interface for Computer Network Defense, Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting – 2014.

[2] Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B.: Towards Understanding IT Security Professionals and Their Tools. In: ACM Symposium on Usable Privacy and Security, pp. 100–111, 2007.

[3] Burns, C. M. , Kuo, J. and Ng, S., Ecological interface design: a new approach for visualizing network management, Computer Networks 43, pp 369-388, Elsevier B. V., 2003.

[4] Burns, C., Putting it all together: Improving display integration in ecological displays, Human Factors 42, pp 224-241, 2000.

[5] Carasso, D. Exploring splunk, CITO Research, New York, USA, ISBN: 978-0-9825506-7-0, 2012.

[6] Cyber Defense and Situational Awareness, Edited by Kott, A., Wang, C. And Erbacher, R. F., Springer, January 2015.

[7] D'Amico, A., Visual Analytics for Cyber Defense Decision-Making, VAC 2011, Washington, USA.

[8] D'Amico, A. and Whitley, K., The real work of computer network defense analysts: the analysis roles and processes that transform network data into security situation awareness. Proceedings of the workshop on visualization for computer security (VizSec 2007), Springer, Berlin, pp.19–37, 2008.

[9] D'Amico, A. and Kocka, M., Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned, IEEE Workshop on Visualization for Computer Security, 2005.

[10] Endsley, M. R., Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1) : 32-64, March, 1995.

[11] Endsley, M. R. and Jones, D. G., Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition, CRC Press, 2004, ISBN 9781420063554.

[12] Franke, U. and Brynielsson, J., Cyber situational awareness – A systematic review of the literature, Computer and Security, 26, pp 18 -31, 2014, Elsevier.

[13] Geers, K., Strategic Cyber Security, CCD COE Publication, ISBN 978-9949-9040-7-5, 2011.

[14] Grégoire, M. and Beaudoin, L., Visualisation for Network Situational Awareness in Computer Network Defence, NATO IST-043 Visualisation and the Common Operational Picture, ISBN 92-837-1149-1 Toronto, September, 2004.

[15] Heer, J. and Shneiderman, B., Interactive Dynamics for Visual Analysis', ACM Queue 10(2), pp 1 -30, February 2012.

[16] http://www.vacommunity.org/vastchallenge2013
[17] Mastering the Information Age Solving Problems with Visual Analytics, Edited by Keim, D., Kohlhammer, Ellis, G., and Mansmann, F. 2010, ISBN 978-3-905673-77-7, http://diglib.eg.org
[18] McKenna, S. Staheli, D. and Meyer, M. Unlocking User-Centered Design Methods for Building Cyber Security Visualizations, IEEE Symposium on Visualization for Cyber Security (VIZSEC), 2015.
[19] Lahmadi, A. and Beck, F., Powering Monitoring Analytics with ELK stack. 9th International Conference on Autonomous Infrastructure, Management and Security, June 2015, Ghent, Belgium.
[20] Lau, N., Jamieson, G. A. and Skraaming, Jr. G., Distinguishing Three Accounts of Situation Awareness based on their Domains of Origin, Proceedings of the Human Factors and Ergonomics Society 57th Annual Meeting, 2013.
[21] Lavigne, V. and Gouin, D., Visual Analytics for Cyber Security and Intelligence, The Journal of Defence Modeling and Simulation: Applications, Methodology, Technology, April 2014. http://dms.sagepub.com/content/11/2/175
[22] Lefebvre J., Grégoire M., Beaudoin L. and Treurniet J., Joint Network Defence and Management System: Concept Document, DRDC Ottawa TM-2003-230, 2003.
[23] NATO 2020: Assured security; dynamic engagement, 17th May 2010.
[24] Paul, C.L. and Whitley, K. Human Aspects of Information Security, Privacy, and Trust, Volume 8030 of the series Lecture Notes in Computer Science pp 145-154, 2013.
[25] Peng, T., Leckie, C. and Ramamohanarao, K., Survey of network-based defense mechanisms countering the dos and ddos problems. ACM Computing Survey, 39(1):3, 2007.
[26] Pirolli, P. and Card, S., The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis, International Conference on Intelligence Analysis, McLean, VA, May 2005.
[27] Rasmussen, J., Mental models and the control of action in complex environments. Mental Models and Human-Computer Interaction 1 (pp. 41-46). D. Ackermann, D. & M.J. Tauber (Eds.). North-Holland: Elsevier Science Publishers. ISBN 0-444-88453-X, 1990.
[28] Rasmussen, J. & Vicente, K. J., Coping with human errors through system design: Implications for ecological interface design. International Journal of Man-Machine Studies, 31, 517-534, 1989.
[29] Rasmussen J., Goodstein L.P., "Decision Support in Supervisory Control of High-risk Industrial Systems," Automatica, vol. 23, .no. 5, pp. 663-671, 1987.
[30] Rasmussen, J. The role of hierarchical knowledge representation in decision making and system management, IEEE Transactions on Systems, Man and Cybernetics 15, pp234-243, 1985.
[31] Rasmussen, J., Skills, rules, knowledge; signals, signs, and symbols, and other distinctions in human performance models. IEEE Transactions on Systems, Man and Cybernetics, 13, 257-266, 1983.
[32] Shiravi H., Shiravi A. and Ghorbani A.: A survey of visualization systems for network security. IEEE Transactions on Visualization and Computer Graphics, Volunme18, Issue 8, pp 1313–1329, August 2012.
[33] Thomas, J. J., Taxonomy for visual analytics: Seeking feedback. VAC Views, May 2009.
[34] Thomas, J. J., Visual analytics techniques that enable knowledge discovery: detect the expected and discover the unexpected. ACM SIGKDD Workshop on visual analytics and knowledge discovery (VAKD 09), Paris, France, 28 June 2009.
[35] Thomas, J. J. and Cook, K. A. (Eds.), Illuminating the Path: The Research and Development Agenda for Visual Analytics, National Visualization and Analytics Center, 2005.
[36] Tufte, E. The Visual Display of Quantitative Information, Graphic Press, Second Edition, ISBN-13: 978-0961392147, May 2001.
[37] Varga, M.J., Winkelholz, C. and Lavigne, V., Application of visual analytics in multi-domain situation awareness, NATO IST-136 Specialists' Meeting on Security Challenges for Multi-domain autonomous and unmanned C4ISR Systems, Lerici, Italy , 21st – 24th March 2016.
[38] Varga, M. J., Winkelholz, C., Träber-Burdin, S. and Varga, C., Chapter 5: Visualization and Analysis for Cyber Situation Awareness, NATO IST-110, Visualization for Analysis Technical Report, 2016. To be published

[39] Varga, M. J., Winkelholz, C., Träber, S. and Varga, C. F., Visualization of Cyber Situation Awareness, NATO SAS-106 Symposium, of Analysis Support to Decision Making in Cyber Defence, Tallinn, Estonia, 9th – 10th June 2014.
[40] Vicente, K, and Rasmussen, J., Ecological Interface Design: Theorectical foundations, IEEE Transactions on Systems, Man and Cybernetics 22, PP 1 – 18, 1992.
[41] Winkelholz, C. Chapter 6: Cyber Defence – Visualizing and Analysing Netflow Logfiles, NATO IST-110, Visualization for Analysis Technical Report, 2016. To be published
[42] Winkelholz, C., Höckling, S., Kruger, F., Günther, H., Flemisch, F., Semling, C., et al. (2013). Human Factors for Cyber Defence - Final Report. Brüssel: EDA.
[43] Wong, W. L., Fluidity and Rigour: Designing Visual Analytics for the Demands of Intelligence Analysis, NATO IST-116 Visual Analytics Symposium, Shrivenham, United Kingdom, 28th – 29th October 2013.
[44] Wong, W. L. and Varga, M. J. Black Holes, Keyholes and Brown Worms: Challenges in Sense Making Human Factors and Ergonomics Society's 56th Annual Meeting, Boston, USA, 22nd – 26th October 2012.