Visualisation for Network Situational Awareness in Computer Network Defence

Mr. Marc Grégoire
Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario, K1A 0Z4
CANADA

marc.gregoire@drdc-rddc.gc.ca

Mr. Luc Beaudoin
Bologik Inc.
157 Champlain
Gatineau (QC) J8X 3R3
CANADA

INTRODUCTION

This document presents some of the requirements and challenges associated with the visualisation for network situational awareness in computer network defence. It raises fundamental questions pertaining to the integration of information and its presentation to the user.

Situational awareness is essential for decision makers to efficiently manage their resources. Situational awareness has historically been associated with aviation security applications, such as air traffic control (ATC), fighter missions, and missile defence. However, the number of studies in the field of situational awareness for new applications has grown significantly in the past fifteen year [4].

The concept of situational awareness involves both a person with his cognitive processes, as well as a situation with various information types and statuses [10]. In a complex environment, which is often the result of growing technology, strong situational awareness can greatly improve the rate and the quality of human decision-making. The cyber domain is one such complex technological environment. However, time and space, as traditionally used in situational awareness, must be presented to the network defence decision maker with new paradigms.

1.0 WHY NETWORK SITUATIONAL AWARENESS?

Computer Network Defence (CND) is a growing field. Computer crimes around the world cost organizations billions of dollars each year [8]. In response, many organisations have stood up Computer Security Incident Response Teams (CSIRT) responsible for ensuring availability, integrity and confidentiality of network services. Their primary challenge is to maintain situational awareness over thousands of network objects and events.

Grégoire, M.; Beaudoin, L. (2005) Visualisation for Network Situational Awareness in Computer Network Defence. In *Visualisation and the Common Operational Picture* (pp. 20-1 – 20-6). Meeting Proceedings RTO-MP-IST-043, Paper 20. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

1.1 Network Situational Awareness and Military Operations

From a military perspective, network situational awareness means knowing the level of threat and the current status of all network assets in support to the military operations.

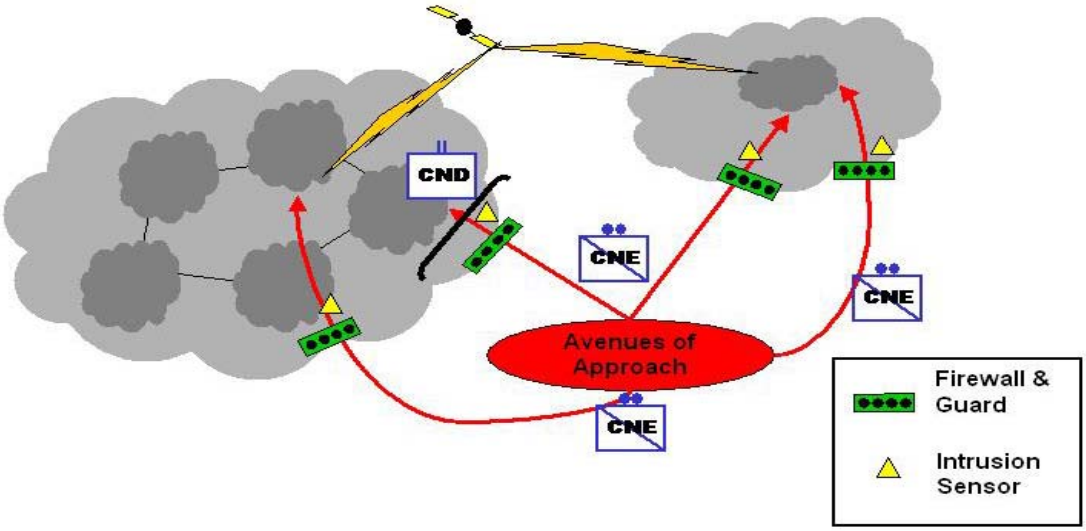

Figure 1: The Cyber Domain as a Battlespace. [9]

This includes awareness of availability, confidentiality, integrity status of the command and control, intelligence, logistics, communications, Enterprise Resource Planning (ERP), information technology (IT) management systems, etc. It also includes the awareness of service providers' infrastructure. This awareness of the security posture includes both physical and cyber domains.

Without a proactive defence of IT services, modern armed forces can be paralysed. Hence, one must consider the cyber domain as a battlespace of its own. Figure 1 presents such a battlefield using common military symbology and Computer Network Exploitation (CNE) and CND as operational units. The casualties suffered in this battlespace can translate into decreased operational capabilities.

1.2 Traditional VS Cyber Situational Awareness

One of the objectives of situational awareness is to allow prediction of the situational state. Normally, this involves object, time and space references. As an example, traditional aircraft situational awareness, from a pilot's viewpoint, may involve the aircraft status, speed, direction, position (Lat, Long, El), the location of other aircrafts, friends and enemies, surrounding landing sites, and the mission [15]. For network situational awareness, the status and topology of the IT infrastructure as a whole is critical. Networking components are usually located using references to the logical architecture. However, these components can also be located using latitude, longitude and elevation references. The interconnections with other networks form the surrounding environment. The IT infrastructure support to the military operations becomes its mission, analogous to the aircraft's mission [2].

Although there are similarities between traditional situational awareness and cyber situational awareness, the latter involves its own particular constraints. Network situational awareness must take into account the high

level of interdependencies between objects in the information grid. These interdependencies can be geographical, logical, or both. At the same time, this complex web reacts at a very rapid pace. The complexity and pace of cyber operations rarely allow for the complete cognitive process to take place before a decision needs to be made. This impacts on the courses of actions available, and hence, on the type of information required. For example, once a network is infected by malicious code, it may be better to assume that the whole network is compromised, and therefore isolate it rather than simultaneously attempting to "cure" infected hosts and prevent the spread of further infections.

1.3 Network Situational Awareness in Support of C4ISR

The Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) model was designed to support the implementation of the Network Centric Warfare [1] concept within military operations. The Network Information Operations section of Defence Research and Development Canada (DRDC) has proposed a Technology Demonstration Project (TDP) in support of this model, which is called the Joint Network Defence and Management System (JNDMS).

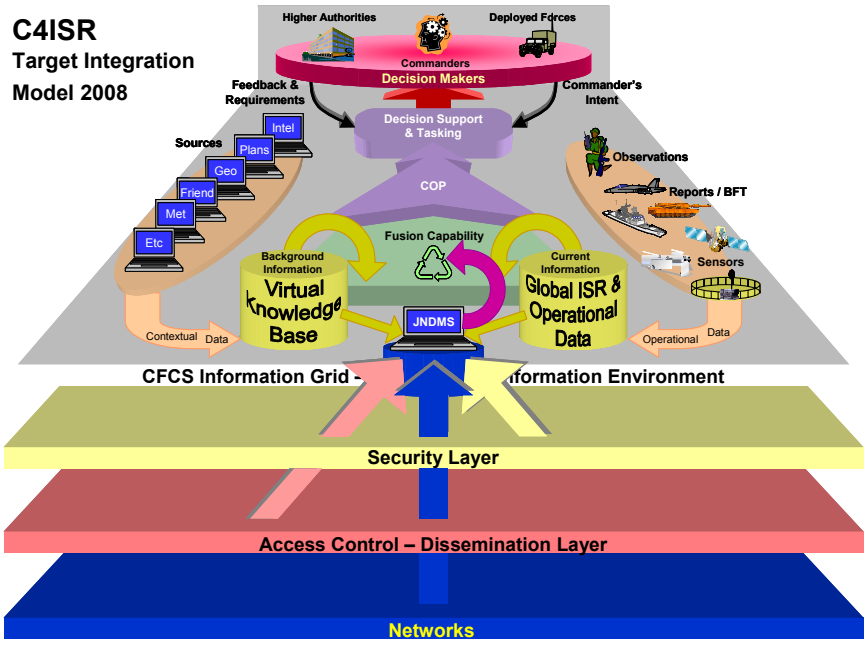

Figure 2: C4ISR Target Integration Model. [5]

The JNDMS TDP will develop a network situational awareness tool for Computer Network Defence. Within the C4ISR model, the JNDMS can be represented as an added layer monitoring the *infostructure* and feeding the fusion capability to provide a Network Common Operating Picture (COP) component to the battlefield COP.

2.0 NETWORK INFORMATION VISUALISATION

Visualisation supporting network situational awareness requires a change of paradigm in terms of speed and complexity. As the interface between human and machine, visualisation of network situational awareness

information is critical. As in many other COPs, different users require different skills to analyse the information presented. Hence, the visualisation must support a large number of cognitive processes (perceptions, comprehensions, projections, resolutions) and contexts (management, security, operations). Some of the attributes pertaining to network situational awareness visualisation are discussed in existing literature [2][3][6].

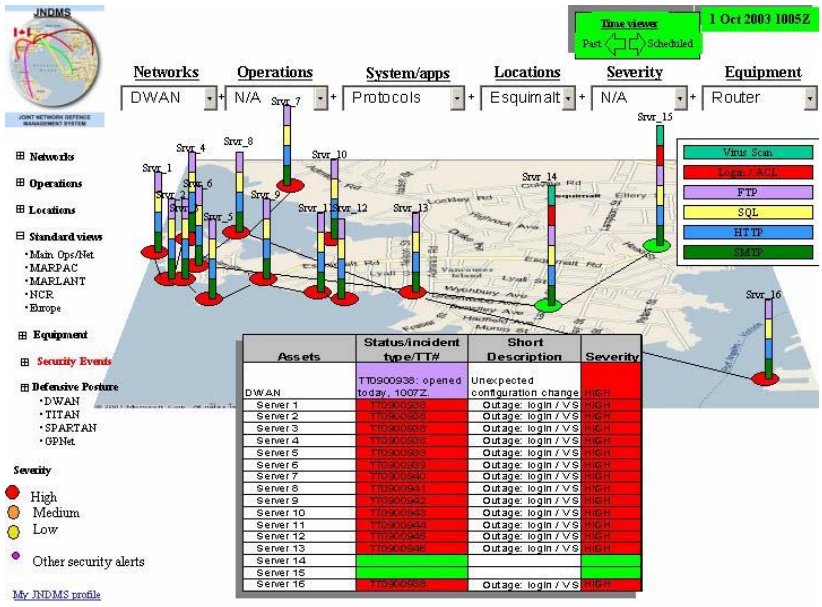

Figure 3: Potential User Interface for Network Situational Awareness. [11]

2.1 GUI Environment

There are a number of user interfaces currently used in the network security management world. Most of them rely on logical and topological network diagrams, as well as database query table reports to display information [7]. This makes sense from a network architecture point of view. However, the logical view of network information makes correlation difficult between cyber events and physical events, such as power outages, storms and explosions. It also ignores the service support agreements, which are generally organised geographically.

The visualisation of asset locations requires a fine level of detail in order to present area assets, such as local area networks (LAN), and connections such as wiring between assets. The area of visualisation varies from thousands of kilometres to a few centimetres.

In order to achieve network situational awareness, both geographical and logical views must be integrated. The use of three-dimensional graphics, as well as different types of multi axis schemas, such as parallel coordinates and scatterplot matrixes [14], can be used to accelerate correlation and assimilation of situational knowledge. Figure 3 shows an example of an integrated view that includes active network links and services, security incidents and geographical information.

The visualisation of networks in support of situational awareness should include the following:

- Geographical view of assets

- Logical view of interconnectivity and dependencies
- Logical view of threat-affected assets
- Logical view of asset configuration (including defensive posture)
- Correlation of IT infrastructure, security events and military operations [11].

3.0 INTEGRATION INTO A COP

Security analysts, network administrators and operational commanders require network situational awareness. In the case of the operational commanders, network situational awareness information should be delivered within existing COP systems, which are generally based on geographic information system (GIS). One of the challenges in doing so is to integrate incompatible data sets. Some of the information modelling standards used for network assets and events include: Common Information Model (CIM) and related directory standards, Incident Object Description and Exchange Format (IODEF), Management Information Base (MIB), Policy Information Base (PIB), ITU-T standards, OSI standards, Vulnerability Description Language (VulnXML), and Simple Network Markup Language (SNML).

A promising model is the NATO General Hub 6 (GH6) developed through the Multilateral Interoperability Program (MIP) [13]. This information model allows some network information to be linked with operational assets and to be fed to C2 systems. Unfortunately, the current model is limited in its ability to integrate the complexity of network security data. Extension to this information model appears to be a valid option to support network situational awareness. As well, the use of extensions to military symbology standards such as MIL-STD-2525 [12] and UK Army Code [16] would allow presentation of this data set.

4.0 DISCUSSION SUBJECTS

Based on our analysis of requirements and technical challenges associated with providing users with the optimal visualization solution in support of network situational awareness, we identified several areas requiring further studies, such as the taxonomy and information standards, the symbology, the physical and logical network assets presentation methods, etc.

Many questions also remain with regards to achieving network situational awareness. How do we define the value of information for network situational awareness? What level of detail is required by each user profile and each cognitive process to achieve network situational awareness? What are the optimal representation methods and interfaces? How can we visualise massive amount of data from networks? What are the real time display requirements? And finally, what are the security issues with integrating network information? These questions should also be answered with consideration to availability and maintenance of the supporting data sets and resulting infrastructure.

5.0 REFERENCES

[1] Alberts D., Garstka J., Stein S., Network Centric Warfare, CCRP, www.dodccrp.org, 1999.

[2] Bass T, Cyberspace Situational Awareness demands Mimic Tradition Command Requirements, AFCEA Signal Magazine, 2000.

[3] Bearavolu R, K. Lakkaraju, W. Yurcik, H. Raje, A Visualization tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks, National Center for Supercomputing Applications (NCSA), University of Illinois at Urbana-Champaign, 2003.

[4] Breton R., Rousseau R., Situational Awareness: A Review of the Concept and its Measurement, DRDC Valcartier TR 2001-220, 2003.

[5] Based on Canadian Forces C4ISR Command Guidance & Campaign Plan, Dec 2003.

[6] D'Amico A., S. Salas, Visualizing Time Patterns and Mission Impact of Cyber Security Breaches, Secure Decision, 2001.

[7] Dodge M., Kitchin R., Atlas of Cyberspace, Addison-Wesley, 2001.

[8] Joint Council on Information Age Crime, Computer-Related Crime Impact: Measuring the Incident and Cost, White Paper, 2003-2004.

[9] Knight R. (LCol), personal communications, 2003.

[10] Lambert D.A. (AS), Bossé E. (Can), Breton R. (Can), Rousseau R. (Can), J.R. Howes (UK), M.L. Hinman (US), J. Karakowski (US), M. Owen (US), F. White (US), Information Fusion Definitions, Concept and Models for Coalition Situation Awareness, TTCP C31 Group, TR-C31-AG2-1-2004, April 2004.

[11] Lefebvre J., Grégoire M., Beaudoin L., Treurniet J., Joint Network Defence and Management System: Concept Document, DRDC Ottawa TM-2003-230, 2003.

[12] MIL-STD-2525B, Common Warfighting Symbology, Department of Defense, 30 January 1999.

[13] NATO Multilateral Interoperability Program Working Group, www.mipsite.org.

[14] Shneiderman B, Visual Data Exploration Access and Analysis, 2nd Annual OCRI Visualization Workshop, 2001.

[15] Smallman H.S., E. Schiller, C. Mitchell, Designing a Display for the Area Air Defense Commander, SSC San Diego Technical Report, 1999.

[16] UK Land Component Handbook, APP-6A Map Symbology, Army Code 71748, 2001.