A Need for Better Network Visualization

Col (Ret'd) Randy G. Alward
RR 3
Lanark, Ontario K0G 1K0
Canada

Randy@ralward.anikast.ca

INTRODUCTION

I hold strong views on the need for Network Visualization. This paper is not scientific, but rather prescriptive of a way forward for the NATO R&D community. There is an urgent need to improve Network Visualization and I present my view of how to proceed herein.

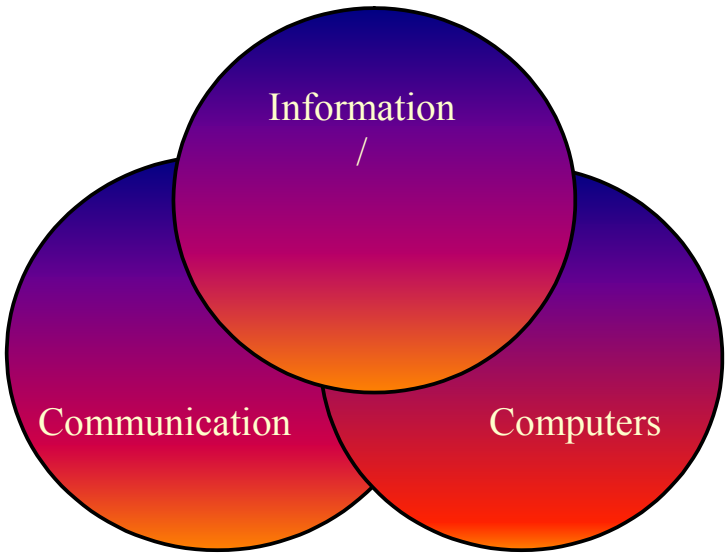
VIEW OF CYBERSPACE

What is Cyberspace?

The advent of the "Information era", many now say revolution, has resulted in its creation.

Consider:

- Communications with near infinite bandwidth shrinking the world into a global village; cell phones, PDAs and wireless notebook computers are pervasive.
- Computers with ever increasing capability in every office and home; everything is 'smart'(er), including your cell phone.
- Explosive growth in information and knowledge; disruptive, non-linear advances in nearly every field of human endeavour.

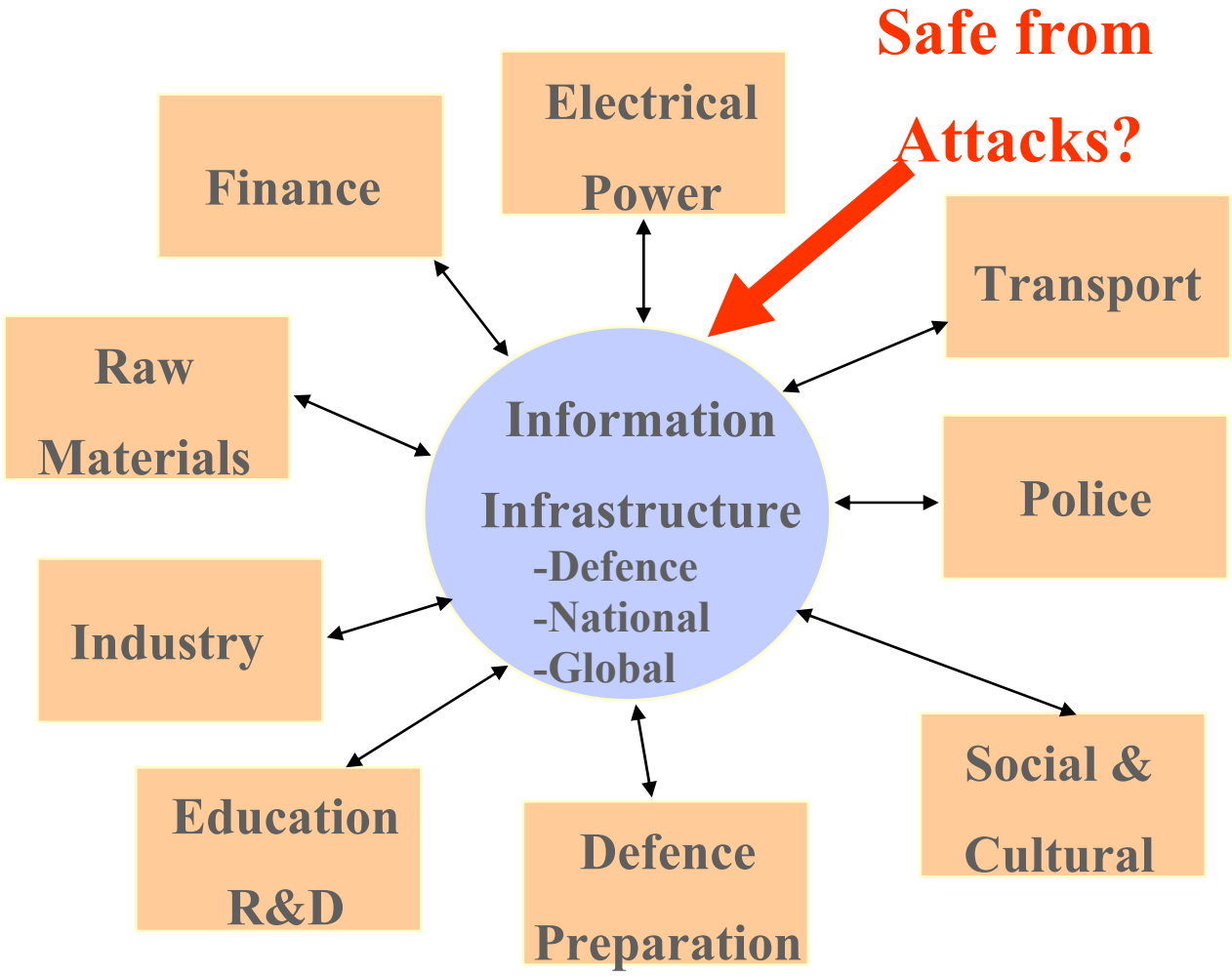


Alward, R.G. (2006) A Need for Better Network Visualization. In *Visualising Network Information* (pp. KN2-1 – KN2-10). Meeting Proceedings RTO-MP-IST-063, Keynote 2. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

The convergence of these three elements creates cyberspace with profound and direct effects on our daily life.

The 'Net' or 'Web' has become so pervasive that we no longer think of cyberspace in terms of its components.

This convergence has led to the creation of an information infrastructure; defence, national and global. I don't believe we can separate them.



It is in the process of revolutionizing the areas you see on this slide. Consider the Internet and its social impact.

Is this infrastructure safe from attack? Consider the North America power outage of 2003 (Ontario, New York state and Ohio) and Canada's ice storm of 1998. The US seems forever under attack, first 'Moonlight Maze' and now 'Titan Rain'.

Clearly we need the best of tools to manage this infrastructure given its ability to adversely impact our nations.

If we are not safe from attack in this new environment, you should be asking why use it.

The answer is simple when it comes to the military; it allows for better decision making and it allows for an increased operational tempo. Work within the adversary's decision cycle.

Indeed, our need for computer networks grows; it has become an essential part of almost every business and we all speak of transformation. Business has gone 'on-line'. Our militaries are transforming themselves to engage in Network Centric Warfare.

Network Centric Warfare, Network Enabled Operations, Network Enabled Capability, Network Centric Operations are the terms our different nations use for the same concept, transforming themselves to take advantage of the Information Age. It is about using networks to speed up and improve the C2 process. It is a disruptive innovation and will evolve with experience, but it has already made phenomenal change in the way we conduct operations, most notable the in the US military.

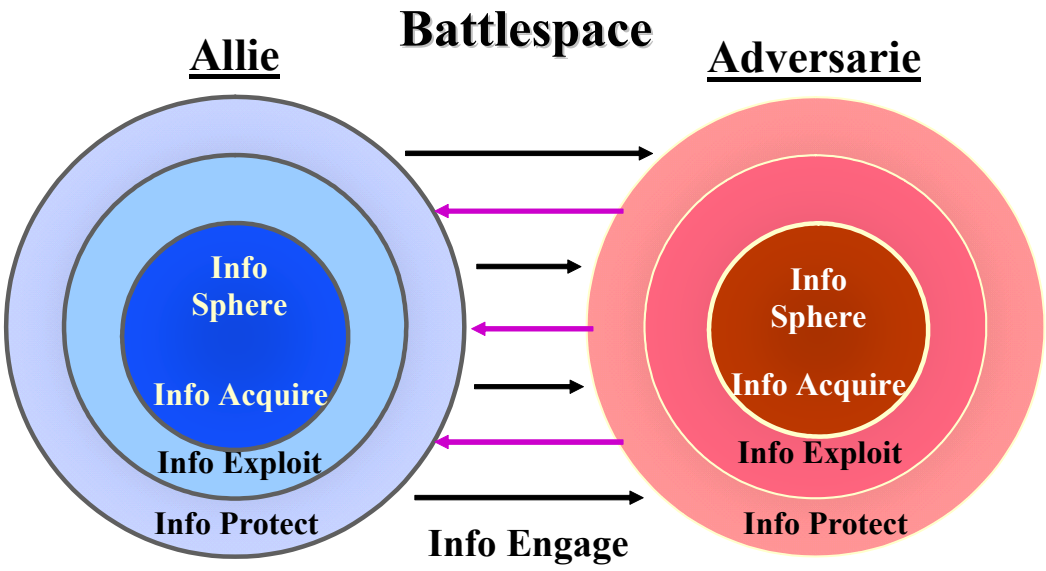
Consider the first and second Golf War. You will recall in the first the extensive use of airpower in advance of the land forces. You did not see that in the second; it occurred simultaneously. That was Network Centric Warfare and it will get better still as we transform and gain experience.

The point in all of this is that we need to maintain our networks in support of operations, and to do that we need to exercise the same excellence in C2 over our networks, over cyberspace, as the army, navy and airforce do over their environment.

Canada's Chief of the Defence Staff recently stated that the delivery of a C2IS able to support Command Centricity and Mission Command, i.e. Network Enable Operations, is one of his top priorities. It should be the top priority of his counter parts in your nations as well. It will do little good to advance NCW if we can not operate and maintain the underlying C2IS. We need better network visualization!

A Paradigm for Cyberspace

We have an Information Sphere; the total of all of our information on all aspects of the operational environment, on opposing forces and on friendly forces. Our adversaries also have an Info Sphere. Hopefully less complete than ours, less accurate, less current.



We want to perform four processes in cyberspace; information acquisition, exploitation, protection and engagement.

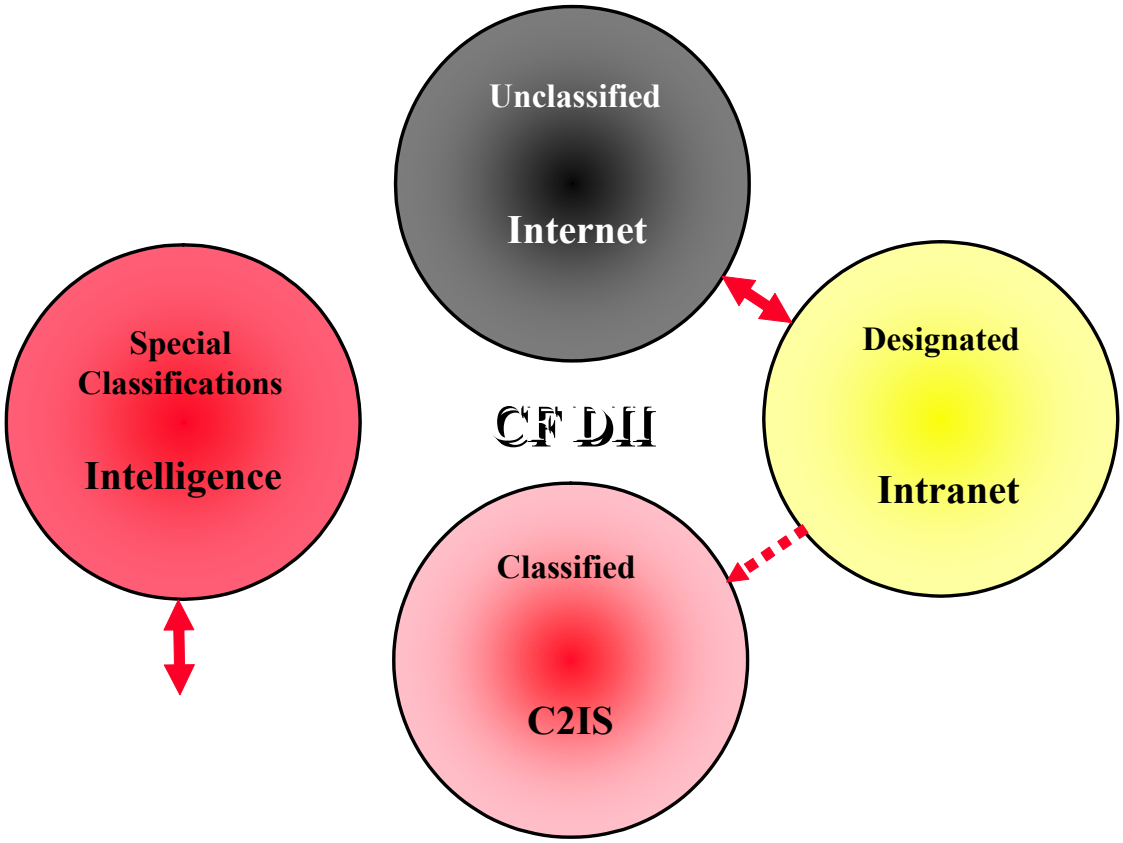
We acquire information from our own staff on personnel and logistics, from intelligence and from sensors to name a few sources.

We exploit the information we possess by exercising effective command and control.

We protect the information from our adversaries for obvious reasons.

And finally we will want to engage our adversaries' cyberspace by breaking through his protection, altering his exploitation algorithms, blinding his ability to acquire information, feed him the wrong information, destroy or corrupt his information.

We need tools to facilitate each of these processes.



That single Info sphere is not a reality today. Our information protection capability is not up to the challenge. Canada can be used as an example, but I suggest it equally apply to each of your nations and NATO.

Instead of an integrated information environment, we have four spheres; an unclassified Internet, a designated Intranet, classified Command and control systems, and special classified networks for areas such as Intelligence.

We have controlled connection between the Internet and Intranet via a gateway, but a great demand for open access.

Network Enabled Operations requires we improve on this situation.

CURRENT SITUATION

What is the current situation in regards to being able to visualize the networks?

We have a logical view of our networks with an indication that data is or is not flowing between routers; green meaning data is flowing and red meaning it is not. This is not an acceptable indication of availability. Is there adequate bandwidth to pass the traffic? Are transactions occurring with applications? Our network operators are happy as long as the indications are green, when in fact we may not be meeting the user's needs. We need a better view of the networks and what is occurring on them.

There is no geographical representation of the network, so the network operations staffs have no idea as to whether an outage impacts an operation or not. How can they prioritize which problem to address first?

They are, in general, unaware that upgrades are being rolled out, which are often the cause of problems.

For all intents of purpose our Network staffs are blind, unable to make timely, prioritized decisions regards network repairs. This is certainly an unacceptable condition for Network Enabled Operations!

REQUIREMENT

Lets now look at some of the requirements regards effective network management.

First, the requirement to know the network state varies in detail with position.

The CIO wants a true view of overall network 'availability'. Are user requirements being met - transactions are being performed; information is flowing in a timely fashion?

The J6 wants a view of the network 'availability' in relationship to current and planned operations. He will want to be able to adjust bandwidth in certain parts of the net to meet intelligence needs for imagery, to prioritize restoral activity, to direct response to network attacks to elements of the network essential to operations.

The System Administrator wants a detailed view of the portion of the network that he is responsible for. availability, maintenance activity, use of bandwidth. He needs to exercise control over his part of the network to establish accounts, re-issue passwords, and a myriad of other tasks.

The Security Analyst wants a view of all security events. Intrusion Detection reports, Anti-virus reports, firewall logs. He wants to be able to adjust the network elements in response to security incidents. He needs these things in real time.

We need multiple views of the network:

- A logical view that shows communications links, routers, servers, firewalls and applications.
- A physical view that overlays the logical view on a geographical representation.

- A transactional view that shows if the various applications are functioning. Is logistics delivering just in time supplies? Are invoices being paid on time?
- An operational view that shows commanders and staff are able to use the networks to gain the advantage that Network Enabled Ops promises. Network staff can prioritize restoral on the basis of operational priorities.

Different types of network activity require different views, different information, and different controls.

The requirements are complex.

RECOMMENDATION TO AN APPROACH TO R&D

I would like to offer you an approach to R&D that will allow you to move your networks to a Network Enabled Operations posture in the shortest time possible with near immediate improvement. I am talking of an approach in which you tightly link your Network Operations Centers, your Defence Labs, your universities, particularly your military colleges, and industry. You might say that they are already linked. I would argue not tight enough. You might say we try but the operator shows little interest. You would be right in general; they are too busy putting out fires. Notwithstanding, I believe you can build a tight and mutually supportive team.

In preparation for this presentation I met with the Canadian Forces Deputy J6 and the Network Operations officers for both their classified networks and intranet. They are frustrated and stressed by their lack of ability to effectively manage their networks and they struggle to make progress.

The network operations and engineering staffs should strive to improve the situation with commercial off the shelf products. Some do, but most don't have the time. It is a slow process and funding is often not available. Network engineering staffs should be providing the tools, but they are often looking for comprehensive solutions that don't currently exist. Again, this is a slow process taking years. I would further suggest that most Network personnel hold a technical view of the network and don't appreciate its operational impact. The bottom line; there is an immediate need for education and quick, shot-term solutions, as well as more comprehensive longer term solutions.

I respectively suggest that R&D staff should develop a close relationship with the network staff, both operations and engineering, gain a sense of the immediate need and work with them to develop better tools for network management. In the short term, R&D staff should integrate some of the cots products in the lab, quickly followed by deployment to the network operations centers. In the longer term R&D staff should develop a more comprehensive solution integrating and promoting development of cots products. The resulting solution should be incrementally delivered to the network operations centers, and also maintained as an operational test bed in the lab. This solution should be continuously improved by R&D staff working closely with the network staffs. As well, shortfalls should be identified that require longer term research. This research could be done in our defence labs, in our military colleges, in universities, in industry with our R&D personnel leading.

An additional benefit to this approach is that R&D personnel would gain understanding of Net Ops and indeed could be called upon to assist in times of crisis. You would also have real-time, live network traffic to work with.

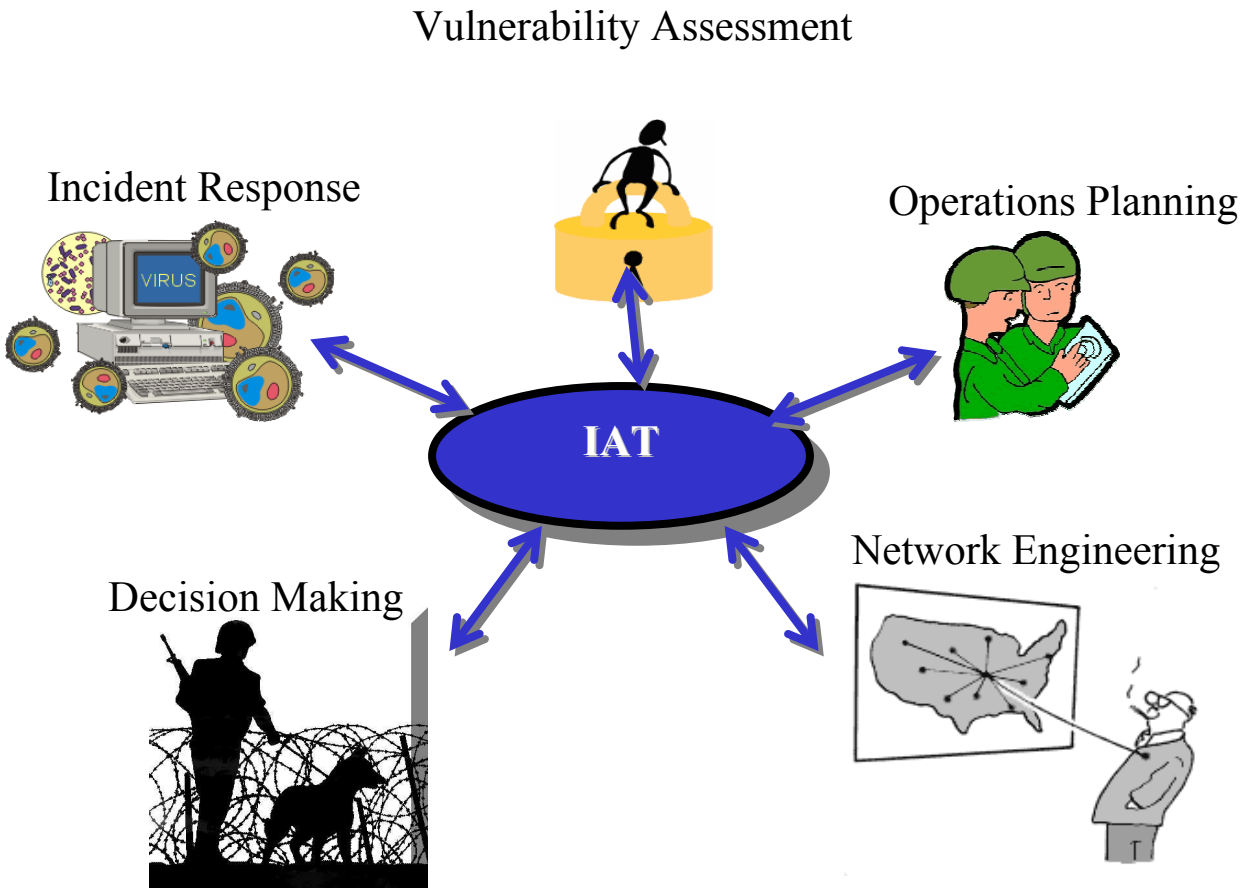
Examples:

The immediate needs of our network operations staff are:

- They need a true view of availability; not just a go/no-go view of the network links. This would allow staff to address issues as soon as the networks fail to meet user needs rather than waiting until the network fails.
- They need basic information, as basic as the name and phone number of the system administrators of the various parts of the network, and it must be kept up to date.
- They need a physical view of the network so they can have a basic appreciation of the networks relationship to on going operations. Networks in Afghanistan are likely important to operations in Afghanistan.
- They need a true view of the network in relationship to operations. They would then be able to give the right priority to the restoration of the network.

Development is required to adequately deliver the capability to meet these needs.

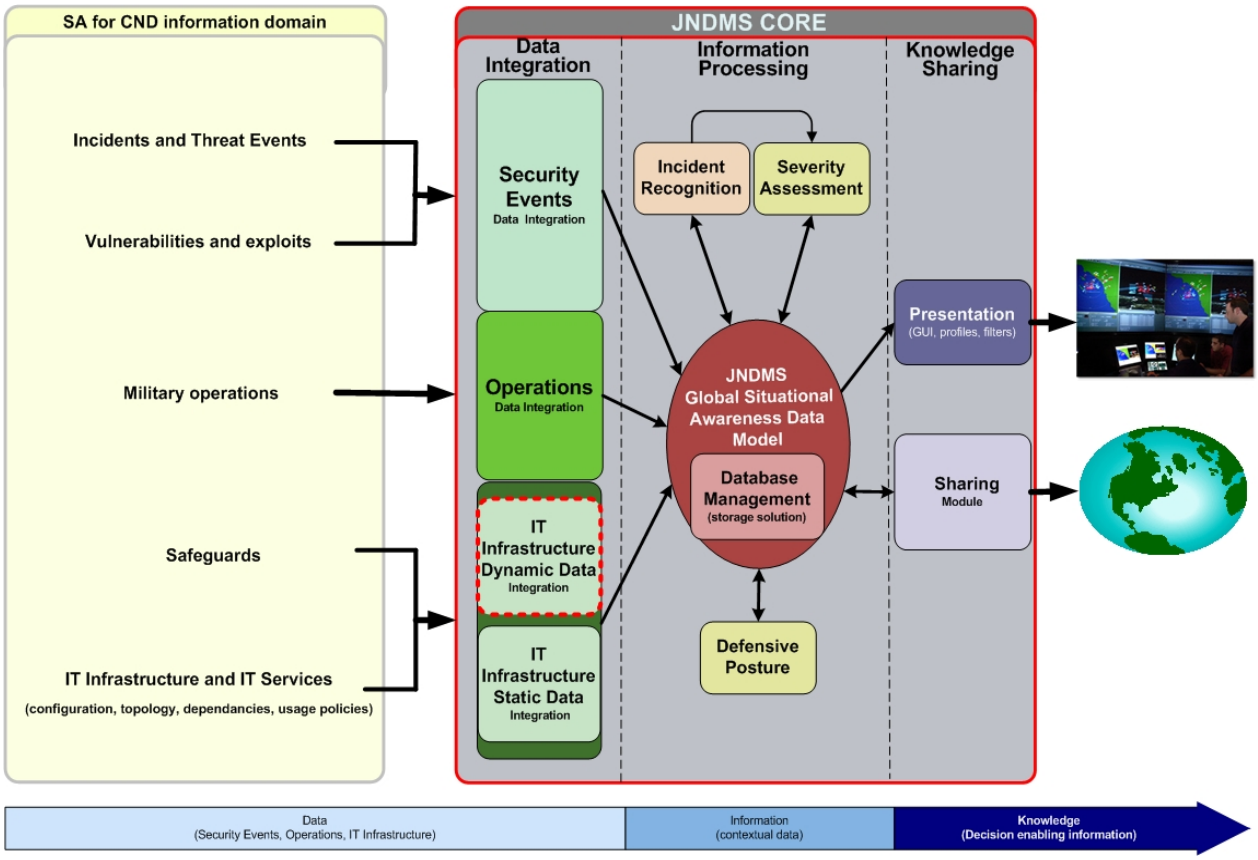
Short term development can and is being used to meet these immediate needs. The Impact Assessment Tool is an example of a short term development project undertaken by the Canadian R&D folks in the Network Information Operations lab. It is a custom application which will allow a network analyst to enter a variety of network information manually, have it processed and produce a report that will facilitate restoral activity. It will regroup related network information relevant to vulnerability, incidents, decision making, and network engineering, producing a report which is pertinent to assessing the impact and risk of network events.



I referred earlier to the network as being a 'battlespace'. I described the network as a cyberspace which we will need to defend from attack. Accordingly, it needs a true command and control system like the conventional battlespaces of land, air and sea. This requires long term development and research.

The Joint Network Defence and Management System is an example of long-term development being undertaken by Canada's Network Information Operations Lab aimed at significantly improving our Network Operations' ability to oversee our networks. In my view, it is the beginning of a Network C2 system. I will pause for a moment to let you absorb the diagram.

JNDMS Architecture



It will be incrementally developed over the next five years, with each increment being rolled out to the NOC as developed. Feedback will be incorporated into future develop, while the NOC gets the immediate benefit of each incremental development.

The lab will retain a copy of the system as a test bed for ongoing R&D. I suggest the Lab and the NOC, and their respective staffs can be fully linked with the lab becoming an advanced extension of the NOC. Imagine the synergy!

As JNMDS develops, research into various aspects will be required. I have listed a few such areas, but I must admit that some are more development than research. The network mapping component is obviously an area for research. The Relational Database component is likely development. We have large amounts of network reference information related to operating systems, programs, vulnerabilities, patches, threats, incidents, people and organizations. This information needs to reside in a structured, relational database readily available to the various network analysts. Prioritization of network restoral tasks requires research; it may be an application for linear algebra. Visualization is a basic component of C2; 'observe'. Cyberspace is more complex and less understood than the traditional physical space of land, sea and air. In fact it you consider the OSI model, it is comprised of seven layers, physical being one; both basic and advanced research is required.

CONCLUSION

I leave you with four points:

- There is an immediate and critical need for advancing network Command and Control
- Progress has been marginal in our Network Operations Centres
- Create a seamless environment across Net Ops Centres and R&D Labs
- Get R&D results into the Ops Centres soonest