Network-Centric Warfare? Homeland Security?

IST-043/RWS-006 Working Group 2 Report

by

Dr. Susan Chipman (US), Bill Cunningham (US), Maj. Christopher Horeczy (CA), Daniel Iaboni (CA), Dr. Erland Jungert (SE), Garth Shoemaker (CA), Vincent Taylor (CA)

Computer, logistics and local social networks are all critical within the context of National Defence and Homeland Security. Each type of network is a potential target for adversaries not only in times of heightened tension but also when the perceived threat level is low. An undetected compromise of a network, affecting the ability of the network to function as expected could have disastrous consequences. Attacks that are detected but whose impact is not understood are equally dangerous. An undetected failure of a network element can be just as catastrophic. ***Either comprehend the network fully or eventually it will not work****.*

DEFINING THE NETWORK

To comprehend a network fully, one must first understand **what is the network**. In other words, one must first know such things as: what is included and what is external to the network; how the network is connected to its external environment and how it is expected to interact with it; how the elements of the network relate to each other and how they are expected to interact; and what is the role of the network with respect to the class of activities and missions the network is expected to support. Regardless of the type of network being considered - e.g. computer network, logistics network or local social network, all the above elements are in play.

All the elements above combine to provide a model of the network. However, to comprehend the network fully, it is not only important to understand the model, but also to know at any point in time how the network is behaving with reference to the model. If one presumes that the network will behave in accordance with the model and one has no hard information to bear that out, the network will eventually fail – i.e. it will no longer perform its allotted functions in an acceptable manner. Thus it is essential that the network be well instrumented so that the relevant information can be gathered and analysed and an appropriate course of action instituted. It is also important to have available up-to-date information (intelligence) about any changes which are occurring in the external environment, or are expected, that might impact the network. In essence, just as for all other battlespaces, network operations requires a command centre supported by appropriate tools. ***However, each type of network (computer, logistics, social etc.), although similar in concept, is very different and operates in its own battlespace!***

NEED TOOLS TO COMPREHEND THE NETWORK

Tools are required that will provide the command centre operator with the status of the network; the protection posture of the network - i.e. the tools, mechanisms, policies and procedures that are in place for the network to assure the integrity and availability of the network and appropriate confidentiality of the network information

Chipman, S.; Cunningham, B.; Horeczy, C.; Iaboni, D.; Jungert, E.; Shoemaker, G.; Taylor, V. (2005) Network-Centric Warfare? Homeland Security?. In *Visualisation and the Common Operational Picture* (pp. WG2-1 – WG2-4). Meeting Proceedings RTO-MP-IST-043, Working Group 2 Report. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

sources and sinks; the impact of internal and external events or activities on the network; and the means by which to restore the network to a known state following a disruptive event.

To obtain the status of the network - i.e. can or can not the network support its missions - tools are needed that will help the command centre understand the network state. This would include: how the network is actually configured; what it is actually doing; and how it is doing it. One particular need is to know what deviations there are from the expected network configuration and network behaviour, what anomolies are evident as well as what changes from the expected are occuring in the external environment that are impacting, or may impact, the network.

Tools are required to: confirm the protection posture of the network and to ascertain whether the actual and expected protection postures are identical; understand the impact of any deviation; and alert the responsible person in an appropriate manner of such deviation.

A command centre can not make intelligent decisions about a network without understanding the impact that events may have on the state and status of the network. Tools are required that will give the command centre a simulation capability to understand *a priori* what effects such events would have upon the network and its behaviour.

When a network needs to be modified or restored as a result of a disruptive event, tools are needed to be able to assess the impact a restorative course of action would have on the ability of the network to perform its mission.

In the various domains, there are a myriad of tools that exist that can extract data from sensors and analyse it against databases to create useful information, but there is no comprehensive tool suite that allows a full understanding of the network to emerge. ***Adequate tools do not exist to comprehend the network fully!***

NETWORK SITUATIONAL AWARENESS

The data generated by the instrumented network (sensors), analysed in association with information from knowledge bases, including intelligence sources and user knowledge, comes together to provide some degree of network situational awareness. At the present state of tool development and network understanding, it is unlikely that this can reach a hundred percent. However, if tools are developed and integrated *with this goal in mind* good network situational awareness can become a reality.

Apart from the development of appropriate collection and analysis tools, the following questions have to be considered: How does network situational awareness change with ones position/role in the network? Are performance expectations clear and reasonable? Are there provisions for measurement and alerting? What is the state of the knowledge bases, “intelligence”, sources of information, means of collection etc., and what trust is inherent in the information? Does the network have an independent control channel? This is important for reducing the potential of acting on compromised data in the event of an attack or failure.

FAULTS, FAILURES & ATTACKS (FFA)

It may not always be easy to tell the difference between a network fault, failure or an attack (FFA). Regardless of the type of network, a FFA can affect network nodes and/or links. Any command centre must have: a means of being alerted to an FFA event; a method of identifying what happened - preferably without further

impacting the ability of the network to perform but still capturing the essential elements of the network situation and its environment around the time of the FFA (the evidence); and support for potential courses of action to mitigate against further network degradation and to enhance recovery.

GENERAL

In summary, computer, logistics and local social networks are all critical to National Defence and Homeland Security, But each is very different and has its own battlespace! Conceptually each can be considered as including an underlying infrastructure, defined by its network topography, topology and functionality, that supports the management, storage and flow of "commodities" into, through and out of the network. Commodities could be be, for example, packets and packet contents in an IT network, or boxcars and freight in a transport network. For each network, one requires not only information about the status of the network topology and functionality but also information about the status of the commodity flow.

The external consumer, be it a military commander or a shipping manager, is primarily concerned with commodity flow and how that affects his/her business. The network manager is concerned with network functionality and availability. The great visualisation challenge is to show how perturbations in network functionality are reflected in commodity flow. Also, since the network cannot be fully instrumented, how fluctuations in commodity flow can be traced back to the causal network abnormality.

It is essential to fully comprehend the network or eventually it will not work. To comprehend the network without tool support would be next to impossible. However, despite the myriad of special purpose tools currently commercially available, an integrated set of requisite tools does not exist in any of the problem domains! Tools are still needed that deal with the status of the network, its protection, the impact of both internal and external events on the ability of the network to support its missions, and also that support its restoration in the event of fault, failure or attack.