Network Intelligence
An Emerging Discipline

LTC (Ret) David E.A. Johnson
The Center for Advanced Defense Studies (CADS)
Washington, D.C, USA
david.johnson@c4ads.org

Newton Howard, PhD
Massachusetts Institute of Technology
Cambridge, MA, USA
nhmit@mit.edu

I. INTRODUCTION
Prior to 9/11, the intelligence process and tools used by our government were primarily directed at known threats with well understood functions and activities. However, with the rising importance of non-state actors and asymmetric threats, threat-focused processes and tools are now directed at known threats whose functions and activities are not well understood [1]. Today’s intelligence environment is characterized by data overload, with the information age exponentially increasing the volume, variety, and velocity of available data [9]. This environment has spawned the development of an entirely new intelligence discipline, Network Intelligence (NETINT).

The objective of an intelligence discipline is to apply sources, sensors, and analysis to provide a decision advantage or to enhance decision confidence. The current intelligence disciplines each arose out of a change in environment and technology to provide a unique perspective on the threat [Finley, 1995]. Like the tale of three blind men examining an elephant, each is focused on an object, not directly on a relationship. Combined by a talented analyst, they can provide great insight. Current recognized intelligence disciplines include: Open-Source (OSINT), Human (HUMINT), Signals (SIGINT), Geographic (GEOINT), Measurements (MASINT), Technical (TECHINT), and Counter Intelligence (CI) [CJCS, 2007]. All of the current disciplines demand requirements officers, collectors and analysts with unique capabilities.

II. LAYERED NETWORK INTELLIGENCE
Today, these disciplines leverage network analysis tools to add value to analytical products and enhance analytical capacity to spot non-intuitive linkages. However, Network Intelligence is a discipline, not a tool set. NETINT provides insight into relationships to build a representation of threat functions and describe the behavior of a system of systems. Data sources include other intelligence domains, as well as the ubiquitous computing environment and social media. Unique sensors can produce population indexing, sentiment analysis, and models of human intent [Howard and Guidere, 2011; Blair-Goldensohn, S. et al, 2010]. Rooted in US Air Force targeting processes during World War II and Army Special Operations targeting processes established during the Vietnam War, Network Intelligence addresses many of the challenges inherent in identifying mechanisms and measuring effectiveness to support Effects Based Operations [CJCS, 2007; Davis, 2002].

The network intelligence analysis process starts with a systems perspective and establishes the status, behavior and linkages of nodes within and between chosen modes. For example, analysis may model relationships between nodes representing individuals and geographic or conceptual modes. Multi-modal analysis can enable the development of a network model for human behavior, while tool-based approaches do not go this far.

Network Intelligence consists of three layers and six components requiring specialized training and education.

![Network Intelligence Layers and Components](image)

Figure 1. Network Intelligence Layers and Components

The data layer contains specialized tools and environments that handle raw inputs. The open-source CASOS/ORA environment contains tools that replicate most of the more expensive vendor-tailored solutions [Carley et al, 2011]. A data management system must be capable of populating node attributes from vast amounts of dynamic written, audio, video, structured, and unstructured data, including data from other intelligence domains. While
several commercial vendors handle “big” data, the real challenge is to sort the data to reliably identify attribute, relational, and ideational data that lead to belief, desire and intent modeling [Scott, 2000]. State-of-the-art data management tools enable analysts to discover non-obvious relationships between discrete nodes in a network. However, these tools are only as useful as the data is reliable and complete. Uncertain environments require qualitative analysis and intuitive inference to evaluate potential threats. A comprehensive NETINT toolkit will allow for quantitative probabilistic analysis while using qualitative detail on individual and group processes, human intent, and the meaning of observed phenomena to supplement incomplete data.

The analysis layer contains tailored analytics and metadata decisions that respond to the intelligence requirements. Meta-data and data mining methodology decisions determine the attributes of nodes and linkages that will feed appropriate analytic tools. The analyst must also understand the constraints and limitations inherent in the analytic products. Thus, a trained analyst could describe the concepts of “centrality” or “density” and their potential usages, as well as where they would be inappropriate measurements [Wasserman and Faust, 1994; Scott, 2000]. Finally, the analyst must integrate analytic output into an analytic product that addresses operational requirements in a useful way.

The requirements layer contains the systems engineering and mode selections that fulfill the requirements of an intelligence question. This question is answered by creating a useful representation of threat functions (a threat process model) that may be queried any number of times and provide a coherent context for responses. The requirements officer must identify the appropriate systems approach. A DIME or PMESII model at the grand-strategic or strategic level of analysis, or a faction, tribe, or organizational model at the operational and tactical levels of analysis would provide the basic requirements framework [CJCS, 2007]. The nature of subsystems will drive mode choices and integration for dynamic, multi-modal social network analysis. Some intelligence questions may find insight in relationships between individuals or objects, but multi-modal approaches link nodes to concepts, ideas and other abstract values as well [Carley, 2008].

The ability to produce all six components requires a view of NETINT as more than a set of tools. The Human Terrain System attempt to provide cultural and social science insight to field commanders is limited by the requirement for embedding with deployed forces and narrowly-defined data sources due to sampling techniques [Hamilton, 2011]. The effort focuses on scientifically defendable approaches and meta-data decisions. Without addressing higher-level requirements tasks, the analytics produced provide specific answers to the questions of a single non-expert customer. These products do not produce a systemic view that can address the needs of many customers. They can, however, provide data to support network analysis. A broader view of NETINT can add relevance to the Human Terrain System effort, shape strategy development, and enhance operational assessment.

III. CONCLUSION

To develop analysts capable of establishing a networks perspective and making the proper choices at requirement and analysis layers requires significant training. At present, there is no Agency specializing in NETINT, though several have programs that deal with analysis of human and computer networks. A number of projects at the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Agency (IARPA) seek to improve our understanding of the behavior and influence of social networks. The Center for Advanced Defense Studies has developed and implemented a NETINT analyst training program that combines OSINT research and data with open source tools [CADS, 2012]. Research interns graduating from this program are currently serving as analysts with the Secret Service and Defense Intelligence Agency.

REFERENCES