Applications of Distributed, Networked Architectures to Port Security

David R. Garvey, Alidade Incorporated

Executive Summary

While the focus of this workshop is how “Network-Centric Operations” applied a to Homeland Security in a New York/New Jersey Port Authority (NNPA) scenario, it seems that the “home game” of stopping hostile agents at US ports is very difficult and expensive. It is much cheaper to stop them at their coast, the “away game.” The US Navy has recognized that "point defense" in air defense is too expensive and never 100% effective. Warships focus on shooting down planes before they launch missiles, and training crew first responders on damage control if the ship is hit, because point defense against launched missiles is the most stressing problem. Analogously, the "away game" of the DoD/CIA piece of national security and the post-incident response seem to be the best return on investment. This may be beyond the current scope, but it is important to keep the complex context in mind.

While DHS is the lead agency for this effort, “Network-Centric” originated in DoD, so elements of recent years of military thought do apply. The phrases “Network-Centric Operations” (NCO) or “Network-Centric Warfare” (NCW) are not well agreed on in DoD or services. What is agreed on is that NCW is an overarching ‘theory,’ NCO is the ‘concept,’ and each service or agency must have a process of bringing theory and concept to reality for ‘tactical’/first-responders. These constitute Tactics, Techniques and Procedures (TTP) of exactly what and how professionals act to conduct “Effects Based Operations” (EBO) to achieve commander’s intent. NCO/NCW and EBO literature recognize the massive front-end cost in time and money of correctly modeling the opponent and the environment in order to induce the desired system outcomes.

The first short term recommendation is that all actors in the HLS architecture must be using the same system model, and that front-end analysis of the linked system of defended assets, potential attackers, and the nonlinear feedback loops connecting them, using network terminology, must be understood. The second recommendation is that US port hubs must be modeled to see what network properties they exhibit. This must include the foreign ports of departure that interact with the US ports of entry, and the network links between them. In this context, “network,” means any general connection of links (usually verbs) and nodes (usually nouns), and is explicitly not constrained to thinking about fiber optic cables connecting computer hardware and software.

DoD has also learned there is a large up-front cost in information infrastructure. This is a “necessary but not sufficient” condition to conduct NCO/NCW/EBO. Recent business literature shows that it is not worth the investment to merely “connect everyone to everyone” without changing business practices. The third recommendation is that all proposals for future architectures must show what new capabilities are being bought that did not exist before. This requires that new methods of costing are used to quantify these investments. These include such recent concepts as “Real Options” on futures markets.

Issue/Problem Statement

The current discussion involves how to apply the concepts of "Network Centric Operations" to a Homeland Security in a maritime port scenario. One of the hardest case is the existing New York – New Jersey Port Authority (NNPA), it is assumed that if we can address that problem, then all others would be solvable by similar methods. This assumption may not necessarily hold since any port, even the largest, must be viewed as interacting via "flows" of commerce with the larger "system of systems" including all ports of entry into the United States, land, sea, air, and even cyberspace.

Another important distinction is that between Homeland (in general, and port in particular) "Security," as opposed to "Defense." The distinction between the two is clearly defined in legal terms in the US Coast Guard Maritime Strategy for Homeland Security. For this discussion, let it suffice to say that the Department of Defense has a support"-ing" role in Homeland Security, and a support"-ed" role in Homeland Defense. Only Homeland "Security" shall be addressed here.

The above distinction should not be confused with the difference between preventative measures prior to an incident, and corrective measures after an incident. This distinction represents an actual "phase change" in the system that involves a drastic change in roles and responsibilities in a short time period. This phase change from "pre-" incident to "post-" incident is analogous to how military operations qualitatively change from the operations occurring prior to commencement of hostilities, to those that occur once hostilities have begun. Complex adaptive forces need to exhibit the beneficial emergent behaviors we see in this transition but more often, and on shorter time scales throughout incident development.

The four "tenets" of NCO are[1]; 1.) a robustly networked force improves information sharing, 2.) information sharing increases the "quality" of information and shared situational awareness, 3.) this quality information and shared situational awareness enables collaboration and self-synchronization, while enhancing sustainability and speed of command, these in turn are the mechanism of advantage for 4.) increased mission capabilities. The initial networking of the force may thus be viewed as a "necessary, but not sufficient condition" to enable further network centric effects. In other words, you must have robust networking in order to achieve Dominant Battlespace Awareness, and then push that out for a Shared Awareness amongst all actors in a force, and obtain Information Superiority against the adversary.

The above four tenets also imply two massive information requirements often overlooked in the proliferating literature on NCO. First, the phenomena of co-evolution with the opponent must be considered. The "blue" (US Homeland Security forces at the federal, state, and local level) side is inextricably linked by nonlinear feedback loops to the "red" (external opponents wishing to do harm inside the US borders) side. Since the

[1] "Network centric Warfare Primer;" at Department of Defense Office of Force Transformation website; http://www.oft.osd.mil/ Winter of 2003
http://www.oft.osd.mil/library/library_files/document_318_NCW_GateFold-Pages.pdf

vast majority of Homeland Security discussion goes on in the public realm of policy debate, what "red" reads in the newspaper and on the internet or watches on TV will influence how their tactics are modified. *If* correctly modeled, *then* this can be used against them. It's the "if correctly modeled" part of the above logical "if-then" statement that is often overlooked.

The National Security Strategy for Homeland Security, The Department of Defense Chief Information Officer (DoD CIO), and the Markle Foundation Homeland Security Taskforce all emphasize the importance of seamless information sharing amongst distributed diverse actors across the entire mission space. In the nomenclature of network analysis, this is a "flow" of information. This is a minimum requirement, but does not, in itself, enable network centric effects. In fact, service studies have now shown the quantifiable effects of "information overload," where more information actually degrades the decision making process.

An important mathematical theorem[2] states that with these multidimensional dynamic boundary constraints, there is no solution that is right for all problem configurations, in fact, there is no solution for which there does not exist a problem set for which a random solution would not have been better. This is known in optimization and search theory as the "No Free Lunch Theorem," meaning there is no "best" solution to fit all cases. The challenge for leadership is to know when to reconfigure to a new solution, and to have built in the potential structure to allow a larger solution space. Also, the ability to reconfigure is a "futures option" just as in the stock market, and that option has an exercise cost. In practical terms, this means the ability to have adaptive Command and Control in a scenario costs money.

The modern port security problem is an example of a classic "complex" system. It is comprised of many diverse elements ("nodes") networked together and interacting ("linked") via nonlinear feedback cycles within the larger graph of nodes and links[3]. This sort of system has been well studied in the natural world in the last 10-15 years in such widely varied fields as; meteorology, evolution, climatology, agriculture, epidemiology, and solid state physics. Over the last 6-7 years, advances in the basic mathematics of network structures with large numbers of nodes, driven by the explosive growth in socio-economic importance of the World Wide Web, have enabled extending methods of complex systems analysis to social systems with real human actors as decision nodes.

A common way to describe these complex adaptive networked systems is by the visualization and mathematics of "networks." In this context, "networks" mean any conceptualized relation amongst elements (nouns) that have action links (verbs) between them, specifically not just the hardware associated with a given computer network.

[2] ``On the Futility of Blind Search: An Algorithmic view of `No Free Lunch'," *Evolutionary Computation* **6** (1998): 109--127.

[3] "Dynamics of Complex Systems (Studies in Nonlinearity)" Yaneer bar-Yam, Perseus Books Cambridge, MA, 1997

Networks have many interesting properties besides just the number of nodes and links[4]. In order to make informed decisions about what types of networks to design, or how we expect to conduct operations on or with networks (e.g. searching the network comprised of cargo containers and the control points they pass through) one must use the proper network model description. Some of the more significant network properties are;

Degree Distribution: How many nodes have how many links?
Real world networks tend to exhibit Power Law distributions.

Largest Hub: How big a component surrounds the most connected node? By rerouting only ~5-10% of the links, this giant component can appear, relocate, and recede entirely.

Average Path Length: How many nodes must be passed through to get to any other node? On the O(log n) for real networks.

Clustering: How many mutual connections are there? If A is linked to B, and B is to C, what is the chance A is linked to C?

Between-ness: How much is one node a "broker" between sections of a graph? Which node is on the most "short" paths?

Path Horizon: How many nodes away is each node "aware" of?
Flows of information experience a "phase change" to increased efficiency when aware of the farthest extent of the network.

Susceptibility: How likely is it that random node removal will seriously degrade the flow on the network? For "power law" networks, they are very resilient to random node removal.

Neutrality: sometimes incorrectly labeled "redundancy," this is the amount of "excess structure" the network has to reroute traffic around a degraded or damaged node. As mentioned previously, this is a futures option, and has an associated cost.

If the flow of commerce through a port obeys the mathematics of these certain "Power Law," "Scale free" or "Small World" class of networks[5], we should be able to tune and design these properties to allow for NCO in the HLS mission applied to port defense. First we need to model the NNPA system as a network, to discern what network structure it has. There are two sides of the competition to be modeled. The flow of commerce, which natural forces try to "optimize" for maximum profit in minimum time, and the C2 system that might better be able to oppose hostile agents wishing to use that flow for potentially disastrous reasons.

[4] "The Structure and Function of Complex Networks," M. E. J. Newman, *SIAM Review* **45**, 167-256 (2003), at http://aps.arxiv.org/abs/cond-mat/0303516 /

[5] Ibid, Newman

How command and control architecture might be distributed to prevent an incident might be very different than how to organize once an incident develops. Analogously, the best way to route traffic for commercial benefit while still searching for contraband or dangerous cargo, before an incident, might be very different than once initial responders are trying to mitigate an incident. These are the richest areas of current network research; how networks grow through "preferential attachment," and how actions occur on networks[6].

Preferential attachment and flows on networks are fertile fields of study because they also examples of the previously discussed phenomena of the "No Free Lunch" theorem and the future options cost of neutral structure in a network. These costs can only be calculated when the mechanism of phase change from one state to another are correctly modeled. Thirty two months after the attacks on 11 September, traditional modeling methods using the simplest types of networks ("random" or "Poisson" at one extreme, "regular" or "lattice" at the other) are all that are used to model either the threat, or the response.

To delve a bit more specifically into the task of searching for hazardous cargo amongst literally millions of containers in this massively distributed complex network, a few more modeling abstractions need to be considered. All nodes in a modeled network are not assumed to be the same "thing" (noun), nor are the actions (verbs) that link them to other nodes, i.e. Containerized cargo (legitimate and contraband), key decision makers (defenders and attackers), initial responders, piers, warehouses, trucks, trains and ships could all be considered "nodes" in the commerce flow network. Observations from a perimeter or remotely (by adversaries), declaration of emergency incidents, inspections, transfer to new modes of transportation, and boardings could all be considered "links" in the commerce flow network.

The chances of finding a specific container you are looking for by either random sampling or by brute force are vanishingly small. This is because the short average path lengths give fewer opportunities for search/inspection, and each one takes some amount of time. Even a small deviation from a "perfect" search of an Area Of Uncertainty (AOU) over millions of individual items to be searched in that AOU results in error margins compounding and chance of successfully finding the contraband item in the AOU fall off exponentially[7,8].

The above assumes, of course that there is not some sort of intelligence cueing to narrow the AOU in time and space. While this is of course always desirable, it cannot be assumed, and does cost time and money that might more effectively and efficiently be dedicated to a novel search strategy. In such a scenario, the best strategy is a smart

[6] Ibid, Newman

[7] "On Battlespace Knowledge" LCDR J. R. Cares (1997) White Paper for the Chief of Naval Operations Strategic Studies Group

[8] "Search and Screening: General Principles with Historical Applications," B. O. Koopman, Pergamon Press, New York, 1980

search of those links passing through the few hubs with high “between-ness,” as defined previously. Also for the foreseeable short to medium term (~8 years), search assets (be they human, airborne, seaborne, or other national technical methods) will still be scarce and a zero sum game of if they’re used for point defense of the Homeland, they can’t be used for active pre-emptive defense forward, which is our stated National Security Strategy signed by the president.

The earlier discussions of network neutrality and event mitigation show great similarity between trying to protect the commerce flow and modern Computer Network defense schemes. Modern computer network defenders know that skilled attackers will go after routers with high network between-ness, they also know that their chances of detecting and preventing the attack are low and shrinking. They focus, therefore on mitigation, and rerouting through neutral network structure once a key node has been compromised by an attacker. The key to the ability to do this is a detailed mapping of the “normal” baseline behavior of the network so that deviations from normality may be detected quickly and worked around[9].

Another key challenge is that the “risk management” of network centric warfare is one of mitigation, on the above assumption that you can’t stop all penetrations, you must be able to mitigate, reroute and reconfigure using neutral structure. The potential worst case scenario of WMD introduced via the commerce flow into a major urban port facility such as NNPA is obviously far more severe than a denial of service (DOS) attack on a computer network (unless of course the DOS attack is part of a coordinated plan for getting the WMD to it’s release point). This is the policy cost assessment that must be done; what level of effort/cost in enabling and training for fluid rerouting of commerce and C2 during and after an incident is “worth it?”

If we assume that maritime commerce hubs (ports) throughout the world (recall that source and destination must be modeled together in a co-evolving system linked by feedback loops) follow some sort of power law distribution of size (as the data seems to indicate[10]) and throughput, possibly even an extreme power law such as the “Zipf Distribution” observed for world wide web hubs, then the primary recommendation is that we explore the plausibility of making the flow network reconfigurable with the characteristics of a “scale free” or “small worlds” network. While the efforts of the US Customs Agency have made headway in compiling data, this data is still not structured in the correct framework (a complex, as opposed to a regular or random, network). This is similar to the problem in the NCO literature of taking “data” and refining it at various “fusion nodes” by the process of “sense-making” to achieve dominant battlespace awareness.

[9] Santa Fe Institute for Complexity Studies Business Network 2003 Fellowship report of Dr. Robert Ghanea-Hercock, BT Exact Technologies, Ipswich, UK

[10] “Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors” US General Accounting Office report to Congress of July 2003.

There would of course immediately be a great deal of resistance to this as there would be large up front costs that would seem prohibitive if judged by traditional industrial Age economics. The desirability of NCO is not in saving money. Modern information age economics has proven that just overlaying Information Technology on top of old processes is not a cost efficient investment. Only when entirely new capabilities become available is it worth it, i.e. increasing the volume of the state space of options.

As stated earlier, information age connectivity between the *"right"* nodes (all nodes is not necessarily desired, and sometimes detrimental. The "right" nodes can only be judged with a correct model) is the necessary but not sufficient condition for networked effects. If the NNPA is still trying to achieve entry level information age connectivity thirty two months after 11 September, then obviously that must be completed before any of these advanced concepts of NCO can be applied. To assume that the US military is done transforming, and has achieved "netcentricity" which others should now emulate would be a grave mistake. As the Office of Force Transformation website (www.oft.osd.mil) states, the DoD is moving towards Network Centric Warfare via the various service and joint roadmaps, it is not there yet.

Large complex port facilities (certainly hubs in the giant component of the greater commerce network) such as NNPA must be modeled as complex adaptive networks. Given that they exhibit the mathematical characteristics of small world/scale-free networks, we can identify the key nodes for any given configuration of flows. When the flows of commerce change due to supply or demand signals, the network structure must be resilient and robust enough to reconfigure itself into the best new configuration for the dynamic boundary conditions.

One of the problems in current discussions is the vast proliferation of seemingly synonymous, or worse, contradictory terms and definitions. Before having interagency discussions, one always needs a calibration of nomenclature for what is meant by "Network Centric Operations" (NCO). According to the Department of Defense, Office of Force Transformation (DoD-OFT) NCO generate increased capabilities by networking sensors, decision makers and operators to achieve:

> Shared Awareness: Elements in a Distributed Networked Force (DNF) have a global concept of commanders Intent, and "Common relevant Operational Picture (CROP)"
>
> Speed of Command: When decision makers have shared awareness, they reach "understanding" quicker, and may then issue their commands quicker
>
> High Tempo Operations: When decision makers have Speed of Command, and all units have Situational awareness, there is much less lag time in actors executing on commander's intent

Greater Effectiveness: This result sin less wasted effort and all units contributing to effective execution of commander's intent in executing Operations to achieve an Effect (see EBO above)

Increased Survivability: Shared Awareness and the CROP allow units to act, not constantly react, bringing their effects to bear first and avoiding enemy points of strength, thus staying alive

Self-Synchronization: Though all units in a DNF may share a CROP, using only local information they may still adapt and show emergent behavior, to "constructively interfere" with the underlying signal of commander's intent

While these are adapted from a purely military context definition, it certainly applies to the high stress missions of Homeland Security whether preventative, investigative, or first responders to an incident.

As discussed previously, the initial networking of the force may be viewed as a "necessary, but not sufficient condition" to enable further network centric effects. It has been identified as the minimum starting point for further advancements by DoD, the Department of Homeland Security (DHS), and private think tanks. These capabilities must be experimented with to co-evolve between developers and users in the field. What "networked effects" are, and as importantly, how to quantify them is absolutely not known yet in the military, much less in the inter-agency law-enforcement and Homeland Security realm.

Mr. John Steinbit, the DoD Chief Information Officer (CIO), explained his Vision of "Power to the Edge" in testimony to the House Armed Services Committee (HASC) in April 2003 as "people throughout the trusted, dependable and ubiquitous network are empowered by their ability to access information and recognized for the inputs they provide." To this end, he states three goals, 1.) Make information available on a network that people depend on and trust, 2.) Populate the network with new, dynamic sources of information to defeat the enemy, and 3.) Deny the enemy comparable advantages and exploit weaknesses.

The National Security Strategy for Homeland Security of July 2002 devotes an entire chapter to "Information Sharing and Systems," listing a five principle approach to developing information systems for HLS, 1.) balance requirements against privacy, 2.) the HLS community must treat federal, state, and local governments as one continuous entity, 3.) information will be captured once at the source, and then used by many different customers, 4.) create databases of record which will be trusted sources of information, and 5.) architecture must be dynamic and continually evolve to stay ahead of threat capabilities. The Coast Maritime Strategy subset of the national strategy staes even more explicitly that; "...Information will be shared in an unprecedented manner by all agencies…"

In March of 2003, the Markle Foundation released Part Two of their report on HLS entitled "Creating a Trusted Network for Homeland Security." They list seven key elements, 1.) information handling must be decentralized and between users according to a network model, 2.) guiding principles should make clear what processes are allowed and which are prohibited, 3.) national strategy should focus on prevention, 4.) establish rules that allow overlapping jurisdictions while still explicitly protecting civil liberties, 5.) take into account that state and local governments and private sector stakeholders will be important contributors, 6.) establish guidelines for use and protection of private sector data, and 7.) citizen/taxpayers must trust the network to protect their civil liberties as well as their lives and livelihoods.

The Markle report suggests an enterprise solution much like what the DoD CIO Mr. Steinbit calls the horizontal fusion portfolio of initiatives. Much is made of the debate between "push" and "pull" architectures, based on whether it is assumed that the consumer knows what they need more than the originator of the information. "Smart pull" is when more information is gathered and moved and stored in better ways so that consumers can find the information they need to complete their missions quicker. The above lists of competing considerations and characteristics show the many dynamic boundary conditions that constrain which network solutions are the "right" solutions for the HLS mission in a democratic open society that continues to pursue free trade while protecting itself against attacks. So given

New Model/Approach

What we want to avoid in our real world complex commerce flow system, is a cascade of overload failures. If in fact the NNPA system responds as a skewed distribution complex network, then attack/removal of key nodes can result in overload and cascading collapse of adjacent nodes.

Perhaps counter intuitively, it turns out that[11] removal of selected links can prevent propagation of the cascading failure. This is somewhat analogous to a firebreak used in wilderness firefighting. What this would equate to physically might be if one cargo handling facility/pier was put out of commission, subsequent "flows" (say for example, ships) were rerouted farther away rather than to maybe the closer alternate facility which would result in overloading and shutting down the alternate facility also.

So the question then becomes, how do we know from our C2 system set-up which nodes or links to remove to prevent node failure percolating through the system? There is a concept of "loading" for both links (the flows, e.g. containers) and nodes (e.g. a given pier offloading facility). This takes us back to step one, accurate modeling of commerce flow through major US ports as a Complex networked system.

[11] "Cascade Control in Complex Networks" Adilson E. Motter, ArXiv preprint dated 7 January, 2004

Selected Bibliography

“A complex systems perspective on computer-supported collaborative design technology” Mark Klein, Hiroki Sayama, Peyman Faratin, and Yaneer Bar-Yam Communications of the ACM November 2002/Vol. 45, No. 11 27

“Cascade Control in Complex Networks” Adilson E. Motter, ArXiv preprint dated 7 January, 2004

“Homeland Security; Information Sharing Responsibilities, Challenges, and Key Management Issues” GAO Testimony Before the Subcommittee on Cybersecurity, Science, and Research and Development and the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, House of Representatives Wednesday, September 17, 2003

“Horizontal Fusion: Enabling Net-Centric Operations and Warfare,” John Steinbit, DoD CIO, “Cross Talk” The Journal of Defense Software Engineering JAN 2004

“Internet’s Critical Path Horizon” Sergei Valverde and Ricard V. Sole
ArXiv preprint dated 15 January, 2004

“Maritime Strategy for Homeland Security” USCG HQ DEC 2002

“Multiscale Complex Systems Analysis of Littoral Warfare” NECSI Report #F30602-02-C-0158 Yaneer Bar-Yam, April 21, 2003

“On Battlespace Knowledge,” LCDR Jeff Cares, USN, Chief of Naval Operations Strategic Studies Group White Paper, 1999

“Optimization of Robustness and Connectivity in Complex Networks”
Benjamin Shargel, Hiroki Sayama, Irving R. Epstein, and Yaneer Bar-Yam1 Physical review Letters 14 FEB 2003 VOLUME 90, NUMBER 6

“Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain” GAO Testimony Before the Committee on Commerce, Science, and Transportation, United States Senate
Tuesday, September 9, 2003

“The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets” The White House, FEB 2003