2009-09-01

Netcentric Warfare Revisited (NCW): It's Origin and Its Future ... Revisited

Gunderson, Chris

rev 9/1/2009

Chris Gunderson

cgunders@nps.edu

831 224 5182

Network-Centric Warfare (NCW): It's Origin and Its Future … Revisited

It has been a decade since Cebrowski and Gartska, and Alberts, Gartska, and Klein published their watershed Network-Centric Warfare (NCW) Naval Institute Proceedings article and book, respectively. Through the lens of hindsight, this paper examines how their theories and predictions have held up. The authors find that the tenets of NCW have proven valid. Despite pro forma policy to the contrary, the US Defense community has substantially eschewed Cebrowski et al. in actual practice. Ironically, Al Qaeda has implemented the principles and achieved an advantage from them. Meanwhile, lessons learned in the 21st Century suggest two subtle improvements to the original NCW theory. First, success at NCW requires instantiating "smart push" of valued information at the right time (VIRT) as a key tactic. Second, success at NCW requires rapid, agile, "network-centric" acquisition conducted literally within the commercial ecosystem of the World Wide Web.

20th Century NCW Hypothesis

Cebrowski and Gartska published their Naval Institute Proceedings article, "Network Centric Warfare (NCW): Its Origin and Its Future," in 1998[1]. Alberts, Gartska, and Stein published their book "Network-Centric Warfare: Developing and Leveraging Information Superiority," which explored the concept in more detail, in 1999[2]. Arguably, these watershed works triggered a mandate for "netcentric[3] transformation" across the global defense community. A decade later, it is fair to ask how their theories and predictions have held up in the 21st Century.

Recall the original Network-centric argument. The global economy has evolved from the "Industrial Age" to an emerging "Information Age." That means that

---

[1] Cebrowski, A., & Gartska, J. (1998). Network-Centric Warfare (NCW): It's Origin and It's Future. *Naval Institute Proceedings , 124*.

[2] Alberts, D., Gartska, J., & Stein, F. (1999). *Network-Centric Warfare: Developing and Leveraging Informatioin Superiority.* Washington, DC: DCRP .

[3] Wikipedia. (n.d.). *Network-centric warfare*. Retrieved July 16, 2009, from Wikipedia: http://en.wikipedia.org/wiki/Network-centric_warfare. Some people define "Network -Centric" and "Netcentric" differently. This paper, per Wikipedia, does not.

Commercial-off-the-Shelf (COTS) technology is evolving to enable ever-more lucrative information collection and processing. This evolving Information Technology (IT) leverages "Metcalfe's Law." Metcalfe's Law says that the "power" of a network is proportional to the square of number of its nodes[4]. Innovative commercial firms leverage the power of networks to achieve competitive advantage. They do that by co-evolving their business processes with rapidly evolving IT. Hypothetically, an agile networked military force that co-evolves its processes with rapidly evolving IT can likewise achieve "information superiority" over a non-networked force. Successful implementation requires developing comprehensive Doctrine, Organization, Tactics, Material, and Logistics (DOTML) that embrace a culture of, and competency in, innovation and collaboration.

Regarding doctrine, organization, and tactics, the approach Cebrowski, Alberts, *et al*., advocated follows:

- Connect military platforms, weapons, sensors, and information sources via modern routable computer networks.
- Co-evolve military processes with rapidly evolving IT analogously to best commercial practice.
- Seek relevant, timely, and accurate information.
- *Self-synchronize* per *commanders' intent* to achieve *asymmetric advantage* through *information superiority* in the battle space. [5]

21st Century NCW Reality

Regarding Material and Logistics, myriad Government watchdog reports agree that the US Defense Community's acquisition process is stovepiped, monolithic, and serial, and is failing to field network-centric capability.[6] [7] [8] [9] [10] Department of

---

[4] More recent studies have questioned whether N-squared or N Log N is the right estimate of the value of the network, but that difference hardly affects our discussion. Cf. "Metcalfe's law is wrong." www.spectrum.ieee.org/jul06/4109

[5] "Self-synchronize,""asymetmetric advantage," and "information superiority" are terms Cebrowski, Gartska et al used repeatedly. "Self synchronize" means independently and innovatively contributing to the enterprise objectives by understanding both the commander's intended outcomes without explicit instructions. "Asymmetric advantage" is military concept traditionally associated with terrain, e.g. having the high ground provides asymmetric advantage against a foe who must advance up hill. "Information superiority" is essentially the high ground of NCW.

[6] Defense Science Board (DSB). (2009). *Report on DoD Policy and Procedures for Acquisition of Information Technology.* Washington DC: GPO.

[7] Government Accounting Office (GAO). (2006). *DOD Management Approach and Processes Not Well-Suited to Support Development of Global Information Grid.* Washington, DC.

[8] GAO. (2008). *2009 Review of Future Combat System is Critical to Program's Direction.* Washington.

Defense (DoD) strategic plans[11] still talk about the "netcentric transformation" that is *going to occur*. So, did Adm. Cebrowski, Dr. Alberts, Mr. Gartska, and Dr. Stein get it wrong?

Al Qaeda: A NCW Franchise

Al Qaeda does terrorism like MacDonald's sells hamburgers… as a global franchise that allows local variations on an iconic brand. Al Qaeda recruiting and training produces exponential growth in qualified membership. Al Qaeda fund raising sustains that growth. Al Qaeda, with its millions of dollars annual budget and its tens of thousands of employees, ties up billions of dollars and millions of employee man-years of its adversaries' resources. Al Qaeda trade secrets are well hidden from those adversaries. Al Qaeda achieves its asymmetric advantage over its much more "capable" adversaries by using the WWW + COTS IT as a lever to achieve information superiority.

Today you can't safely assume that an adversary will not be effectively networked. The gigantic and ubiquitous World Wide Web (WWW)[12] -- including the associated Internet infrastructure and COTS IT -- provides tremendous power to any "force" that cares to tap in. Certainly Al Qaeda's innovation in its battlespace has demonstrated how the power of COTS IT + WWW can generate information superiority.[13] Al Qaeda's semi-autonomous, innovative forces self-synchronize , i.e. they all understand their commander's intent and act independently, but collaboratively, to bring it about. They leverage relatively small resources against exquisite information superiority to inflict asymmetrically large damage to their adversary. They use WWW + COTS IT as their Global Information Grid. Further, Al Qaeda tactics, techniques and procedures (TTP) continuously co-evolve as COTS IT evolves, thus realizing the adaptive evolutionary behaviors that Cebrowski, Alberts, *et al.* advocated for "Blue Force[14]". Hence, we might consider "COTS IT + WWW"

---

[9] GAO. (2008). *DoD Needs Framework for Balancing Investments in Tactical Radios.* Washington:

[10] GAO. (2006). *DoD Needs to Ensure That Navy Marine Corps Intranet is Meeting Goals and Satisfying Customers.* Washington DC: GAO.

[11] DoD Chief Information Officer (CIO). (2008). *DoD Information Management and Information Technology Strategic Plan 2008-2009.* Washington: OSD.

[12] The WWW is the collection of accessible content and computer applications available over the Internet communications backbone.

[13] Martin , A. *Al Qaeda- A Lesson in Networked Warfare?* Canadian Forces College (CFC) . Toronto: CFC . Royal Air Force Wing Commander Martin explains how Al Qaeda uses the Internet as its Global Information Grid to achieve asymmetric advantage through information superiority.

[14] "Blue Force" is a traditional term for the "good guys" in any military scenario.

as a benchmark of the minimum network-centric capability required to achieve *information parity*[15] with a generic adversary in the 21st Century. Call this benchmark the "adversarial network-centric baseline. "

Given that any adversarial force in the 21st Century will certainly be networked, the issue becomes how one networked force can achieve information superiority over another. Metcalfe's Law – as interpreted by Cebrowski, Alberts, *et al*. -- implies that the force that best uses its networked connectivity to access relevant, timely, and accurate will become the most "powerful." Al Qaeda's success with COTS IT + WWW gives credence to that argument. However, in view of the lessons learned in the first decade of the 21st century, this straightforward application of Metcalfe's law seems incomplete in at least two respects.

- Not all nodes are equally powerful. Specialized private nodes, provisioned amidst the generic nodes of the larger public network, can provide asymmetric advantage to those with access to them.[16]

- *Information processing capability is a limited resource*. "Information overload[17]" brings about diminishing returns for more and more data. Metcalfe's Law applied to large networks makes the volume of data -- even data filtered for relevance, timeliness, and accuracy -- effectively unlimited. More efficient use of processing capability – especially human processing capability – can provide an asymmetric tactical advantage over adversaries hindered by the *fog* of info glut. [18]

Accordingly, an inferred military strategy to achieve NCW information superiority would have three parts:

1. Assure a minimum of Blue Force network-centric parity with adversaries: adopt and adapt COTS + WWW and co-evolve Blue Force TTP with COTS + WWW evolution.

2. Deploy powerful specialized Blue Force nodes designed to leverage and enhance the generic capability available via COTS + WWW. Employ best available methods and tools to protect these nodes and assure their information availability and integrity.

---

[15] "Information parity" as compared to "information superiority."

[16] Consider how many commercial websites have different levels of access. Some services are free; others you pay for. The services that you pay for -- say your on-line banking services and consumer reports -- are protected through a credentialing process. The protected services provide you more power in your personal network-centric activity like shopping on line.

[17] "Information Overload" per Wikipedia. Generally excess information makes processing difficult.

[18] Denning, P. J. (2006). Infoglut. *Communications of the ACM , 49* (7), 15-19.

3. Assure availability and use of valued information at the right time: employ best tools and practices to enhance Blue Force information processing efficiency.

In comparison, the US Defense Community's chosen approach to achieve NCW information superiority for Blue Force in the 21st century has the following corresponding three parts:

A. Build specialized Blue Force capability[19]: use commercial IT paradigms to develop proprietary IT incrementally and evolutionarily; adapt legacy military systems so they communicate using more modern routable proprietary military networks.

B. Lock down Blue Force[20]: rigidly isolate Blue Force networks from the WWW; reproduce generic COTS capability that is available on the WWW by developing proprietary capability and deploying it on proprietary networks.

C. Make all Blue Force data "discoverable" to Blue Force[21]: post all data collected by Blue Force provider-nodes in specified formats; task Blue Force consumer-nodes to find and "pull" timely, relevant, and accurate data.

US Defense Community Saying-Doing Gap

Parts 1 and 2 of the inferred 21st Century NCW strategy are consistent with Cebrowski, Alberts, *et al.* Part 3 is arguably not quite consistent. Parts A & B of the US Defense Community approach contrast starkly with 1 and 2. However, part C is exactly consistent with the Cebrowski, Alberts, *et al.* See figure 1.

---

[19] Department of Defense (DoD). (2008). DoD Instruction 5000.02: Operations of the Defense Acquisition System. DoD.

[20] DoD. (2002). DoD Directive 8500.1, Information Assurance.

[21] DoD. (2004). DoD Directive 8320.02 Data Sharing in a Net-centric DoD.

Implied 21st Strategy vs. Actual Practice, re 20th Century NCW Theory

		Consistent with Cebrowski & Alberts, *et al*?	Inconsistency
21st Century NCW	1. Embrace COTS + open WWW & co-evolve TTP	Yes	
	2. Develop and deploy security services & specialized capability on the open WWW	Yes	
	3. VIRT smart push data strategy	Not quite	Addresses info overload issue. Burdens data/ svc providers to determine & deliver actionable info per pre-defined CCI.
Actual Practice	A. Embrace commercial techniques to develop specialized capability	No	Focus is on technology per se rather than on co-evolving with whatever COTS emerges.
	B. Lock down private military networks	No	Prevents leveraging Metcalfe's law. Precludes Blue Force cross-domain collaboration.
	C. Smart pull data strategy	Yes	

Figure 1: Implied 21st Century Strategy for Deploying Netcentric Capability vs. Actual Defense Community Practice compared to the original NCW theory of Cebrowski & Alberts *et al*.

The paragraphs below discuss the significance of these various consistencies and inconsistencies.

Cebrowski, Alberts, *et al.* argued against focusing on technology. Their principal aim was not to acquire net-enabling and net-enabled technology itself. NCW advances by agnostically consuming whatever appropriate technology it can find. Specifically, they urged DoD to exploit the new business value of the new technology as fast as the best commercial enterprises do. In other words, collaborate with technology providers to acquire and rapidly assemble capability and innovate in ways that provide an asymmetric advantage to Blue Force. That is, fielding network-centric capability requires a network-centric approach to acquisition.

However, the US Defense Community has chosen not to perform network-centric acquisition. Rather, defense policies and programs have embraced trendy IT paradigms like "Service Oriented Architecture" (SOA) as a means to field capability within the legacy stovepiped, i.e. anti-netcentric, acquisition process.[22] These

[22] Defense Science Board. (2009). *Report on DoD Policy and Procedures for Acquisition of Information Technology.* Washington DC: GPO.

policies and programs have not embraced the underlying business models that make paradigms like SOA successful: *i.e.,* re-using off-the-shelf capability to deliver rapid incremental improvements and leveraging the massive economy of scale of the WWW.

Cebrowski, Alberts, *et al.* predicted that the adversarial force of the future might very well be non-state actors such as terrorist groups. They predicted that these actors could engage Blue Force, via NCW, and use information as a powerful weapon. Ironically, Alberts *et al.* even used terrorist access to weapons of mass destruction as a metaphor. Alberts *et al.* explained that the force that invents the new war-fighting method is often not the force whose innovation successfully implements it. Sadly, that turned out to be the case. Al Qaeda has applied NCW to achieve asymmetric advantage over Blue Force through information superiority.

Cebrowski, Alberts, *et al.* explained how the concept of "battlefield" must expand to "battlespace" and even more broadly to "mission space." They said NCW requires that the concept of "space" must include virtual cyberspace as well as concrete terrestrial space. They predicted that the US Defense Community would increasingly concern itself with "Operations Other Than War" (OOTW.) They observed that the extent and value of publically available data sources would often surpass military sources. Hence, they said, the boundaries between civilian and military activity would blur. It seems they got all this right.

Traditionally, Blue Force has trained, equipped, and deployed its warriors to engage and defeat the enemy by exploiting the *terrestrial* terrain the enemy occupied. Per the arguments of the preceding paragraph, NCW implies that Blue Force should now also train, equip, and "deploy" its warriors to engage and defeat the enemy by exploiting the *virtual* terrain that the enemy occupies.

Today, the Internet and WWW is the virtual terrain that the enemy occupies. However, Blue Force has chosen not to train, equip, and deploy its warriors to engage the enemy there. Blue Force has chosen to isolate its warriors in a gated virtual backyard.

The US Defense Community has three main routable networks[23]: JWICS is classified TOP SECRET; SIPRNET is classified SECRET; NIPRNET is unclassified. These circuits are all Internet Protocol (IP) "intranets." That means they use the same technology as the Internet but are not directly connected to the Internet. Blue Force also has several small intranets that support various military multi-national coalitions. Generally those intranets are classified SECRET. Blue Force classified intranets are

---

[23] Routable, or "cloud," networks use protocols such as Internet Protocol (IP) to route data packets from any node to another, asynchronously, and without pre-existing arrangements. Thus, routable computer networks lend themselves to supporting the *ad hoc*, on demand, nature of NCW. Blue Force also has various stovepipe point-to-point tactical links and push-to-talk radios. They are not routable networks, *i.e.* they are not inherently netcentric, but are part of the cyber missionspace.

completely disconnected from the Internet and from each other. The NIPRNET uses gateways and firewalls to gain heavily restricted connectivity to the Internet. All nodes on the NIPRNET are identified by a ".mil" suffix to their Uniform Resource Identifiers (URIs).

We can think of the sum of the military networks as the Blue Force cyber *mission space*. SIPRNET and the coalition intranets are generally the only routable networks used by members of Blue Force who are participating in, or supporting, combat missions. These SECRET intranets, therefore, constitute the NCW cyber *battlespace* for most Blue Force warriors[24]. Clearly the number of nodes on the DoD private networks and volume of their content are orders of magnitude less than found on the Internet and WWW. So, based on Metcalfe's Law, the power of the networks in the Blue Force missionspace is nowhere near that of the adversarial network-centric baseline.

Obviously, the US Defense Community has chosen to cordon off its networks to protect them and their content from intrusion and denial-of-service attacks. Certainly there are legitimate reasons to lock down some data and some networks -- small private intranets can be very useful for local, non-network-centric activity. Further, good balanced need-to-protect *vs.* need-to-share security policy is as consistent with NCW as it is with any other war-fighting paradigm.

However, if successful NCW against a globally distributed adversary is the goal, does it make sense to restrict Blue Force cyber activity to small private intranets? Given that goal, what constitutes balanced need-to-share *vs.* need-to-protect policy?

The large majority of content on classified intranets is not classified. Similarly, the large majority of content of the NIPRNET is not particularly sensitive. Meanwhile, Blue Force denying its members access to the WWW is tantamount to Blue Force conducting a deliberate denial-of-service "friendly fire" attack on itself.

Further, the ".mil" suffix, which only exists on US Defense community networks, is literally a conspicuous bulls-eye that helps adversarial hackers aim at Blue Force cyber targets. More bad news is that those hackers can, and do, hide amongst hundreds of millions of innocuous ".com," ".org," ".net," etc. addresses.

Further still, if we define "Blue Force" as the US Defense Community plus all coalition members, there is no existing cyber battlespace common to all of Blue Force. By contrast, all members of Al Qaeda share common cyber battlespace. Common cyber battlespace is a necessary condition for success in NCW as espoused by Cebrowski, Alberts *et al.*

---

[24] Office of the Secretary of Defense (OSD.). (2003). *Information Operations* (IO) Roadmap. Washington: OSD. This de-classified, but heavily redacted, document discusses "Computer Network Attack" by DoD. Presumably some elements of Blue Force indeed engage the enemy in his own cyber terrain. In our paper, we claim that the bulk of the members of Blue Force are not doing that routinely.

Here again, it appears that Blue Force's adversaries have proven the validity of the Cebrowski, Alberts, *et al.* NCW principles. Blue Force has, again, deliberately chosen not to apply the NCW concepts they espoused.

20th Century NCW Theoretical Gap

Although Al Qaeda has generally validated their NCW predictions, the evidence of the last decade indicates that Cebrowski, Alberts, *et al.,* might have missed, or at least not explicitly explained, two concepts critical to the success of NCW in the 21st Century: (1) network-centric semantic interoperability; (2) network-centric acquisition business model.

Semantic Interoperability is the ability to usefully exchange data among distributed collaborators. Alberts *et al.* said:

> "As in the commercial sector, information has the dimensions of relevance, accuracy, and timeliness. And as in the commercial sector, the upper limit in the information domain is reached as information relevance, accuracy, and timeliness approach 100 percent. Of course, as in the commercial sector, we may never be able to approach these limits…"
>
> "…While the Information Age will not eliminate the fog and friction of war, it will surely significantly reduce it, or at the very least change the nature of the uncertainties…."

Experience in the 21st Century does not appear to support the prediction that the fog and friction of war would be reduced by the existence of a powerful ubiquitous computer network and instant access to hundreds of millions of data sources. Quite the contrary! In fact, the information age has made huge volumes of relevant, accurate, and timely information about any particular subject amazingly available and discoverable. The issue is that processing mountains of *potentially* useful data is tantamount to succumbing to the fog and friction of information war. In other words "information overload" is equivalent to "fog of information war." [25]

It does appear true that "… the Information Age will … change the nature of uncertainties…" In the Industrial Age, battlefield uncertainties came from a dearth of data to process. Data-processing –to-decision windows were on the order of hours to days. In the Information Age, additional cyber battlespace uncertainties come from too much data to process. As Alberts, *et al.,* explained, data-processing-to-decision windows in the Information Age are on the order of seconds to minutes.

---

[25] Hayes-Roth, F. (2007). Getting ahead of the Avalanche: How everyone can benefit from a near-infinite amount of technology. MESDA's 15th Annual Conference, Maine's Software and Information Technology Industry Association.

Overcoming the fog and friction of information war, then, requires Tactics, Techniques, and Procedures TTPs that preserve warrior-processing time for making good decisions quickly. Good NCW decisions achieve asymmetric advantage through superior information processing. Define "significant bits" to mean "decision-quality information." Under that definition, significant bits are those that would change critical assumptions associated with planned actions. In other words significant bits describe critical conditions of interest (CCI) associated with particular desired outcomes.

Given the known unmanageability of 21st Century data volumes, NCW TTP should not task front-line warriors to *seek* relevant, accurate, and timely data as suggested by Cebrowski, Alberts, *et al*. "Relevant" means "pertinent to mission profile". Why waste precious warrior processing time seeking and evaluating merely r*elevant* data bits? It's the *significant* bits operators should process.

Rather, NCW TTP should task warriors to continuously revise and publish their current decision parameters, *i.e.* their CCI. Then warriors can leverage superior numbers and quality of Blue Force nodes to mitigate the fog and friction of information war. That is, they can task the multitude of Blue Force supporting nodes to seek and deliver s*ignificant* bits, and only significant bits, according to their warrior-specified CCI. [26]

Network-centric acquisition is rapid, adaptive, distributed creation, procurement, and delivery of net-enabling capability. Cebrowski, Alberts, *et al.,* suggested Blue Force should use industrial best practice -- but only as a guide. They emphasized that warfare would forever remain much different from industry. They discussed how specialized military sensors, platforms, and weapons should be networked *analogously* to the way commercial industries network their business systems. Their implied truism was that military networks would have distinctive functions, and thus should remain distinct from commercial networks. They at least implied that the military network-centric acquisition should occur in parallel to COTS IT + WWW evolution writ large. In other words, they seemed to envision acquiring a specialized military version of the Internet + WWW to ride on private military intranets.

Army engineers can build a bridge across a river in the middle of a raging firefight. Army engineers have the resources available for that specialized mission because the Army has the good business sense to simply re-use public roads and bridges for the overwhelming bulk of its generic terrestrial transportation.

Likewise, success at information warfare in the 21st Century requires treating NCW

---

[26] Hayes-Roth, R. (n.d.). *Valued Information at the Right Time (VIRT)*. Retrieved July 17, 2009, from NPS Faculty: Rick Hayes-Roth: http://faculty.nps.edu/fahayesr/virt.html

exactly as a business.[27] With all due respect, it seems a bit of a conceit to treat it otherwise. On one hand "business" does not equate to "for profit." Good "business models" optimize return on investment for the organization's mission…period. On the other hand, the bulk of the members of the US Defense Acquisition community, namely defense contractors, are certainly in a for-profit business. Those contractors should compete on the basis of value added on top of the adversarial network-centric baseline.

With the benefit of a decade of hindsight, maintaining large private military networks now appears to be a sunk cost decision.[28] Sunk cost arguments nearly always emanate from bad business decisions. After all, modern routable networks do not have distinct functionality. They are designed to be utterly generic, universally useful, infrastructure. The Internet is truly analogous to the global public transportation network in that regard. Why shouldn't the US Defense community leverage the Internet in the same way it leverages the scale of the global public transportation network?

Given its limited resources and the staggering rate of change in the WWW+ COTS IT landscape, the US Defense community can't possibly keep pace using a parallel proprietary development strategy. Therefore, the only possible way to perform network-centric acquisition is to join and invest in exploiting the massive, distributed, and networked COTS ecosystems… as a peer. COTS-based development, or even buying COTS, is not the same thing as joining and investing in the COTS ecosystem as an industrial peer. [29]

It would appear that the path to NCW success in the 21st Century is to treat network-centric acquisition as an operation other than war (OOTW). Blur the distinctions between civilian and military activity. Join and gain the trust of the WWW + COTS IT community by engaging in good faith on their terms. Help them improve their basic infrastructure. Encourage them to innovate in ways that are consistent with good global cyber security.

Once again, the analogy of military best practice in terrestrial space applies to cyber space.

---

[27] US Department of Education . (1996 , January 3). *Clinger-Cohen Act* . Retrieved July 16, 2009, from ED.gov: http://www.ed.gov/policy/gen/leg/cca.html. Indeed, the Clinger-Cohen act requires that government procure its IT *exactly like* the best commercial practioners do.

[28] Pierce, T. C. (2002, May). Sunk Costs Sink Innovation. *Naval Insititute Proceedings , 128* (5). The "sunk cost fallacy" is the common, fatal, mistake of allowing an existing investment obfuscate what is necessary to succeed. Captain Pierce explains the sunk cost fallacy in context with a particular Navy information system.

[29] Denning, P. J., Chris, G., & Hayes-Roth, R. (2008). Evolutionary System Development . *Communications of the ACM , 51* (12), 29-31.

Closing the Gaps

The NCW ideas of Cebrowski, Gartska, Alberts, and Stein have been validated, indeed profoundly so, by their successful instantiation by Al Qaeda. Yet, despite myriad policies *mandating* net-centricity as a transformational tenet, the US Defense Community continues to *behave* anti-netcentrically – at least with respect to how it acquires its warfighting capability. It seems policy is not the issue. Behavior is the issue. Network-centric behavior, per Cebrowski, Alberts, *et al.,* is independent-yet-collaborative, decentralized, bold and innovative. Therefore, if the US Defense Community hopes to achieve its NCW objectives, it needs its distributed expert members -- especially those involved in acquiring capability -- to behave boldly, collaboratively, and innovatively.

There are also at least two difficult technical challenges that bold, innovative, collaborative capability developers must overcome:

- Information Assurance (IA). Federate across networks on demand, *i.e.,* dynamically create and collapse private network enclaves embedded in the larger public Internet. "Build in" assured security while deploying these federating technologies and methods. It is too hard and too expensive to "bolt on" security later.

- Semantic Interoperability[30]. Manage the "information overload" issue, *i.e.,* deliver critical information to critical nodes in time to provide information superiority.

Modern COTS IT paradigms such as SOA, "Open Source Software", and "Cloud Computing," "Semantic Web," etc. can help overcome the challenges if applied with sufficient scale and appropriate business models. However, it is unlikely that these COTS approaches will deliver capability sufficiently robust for the most stringent military applications without intelligent intervention by the military. That is, to play its role well in the network-centric eco-system, the US Defense Community must incentivize incremental COTS IT development in the right direction. Military procurements should fund and certify COTS IT providers to develop assured, secure, semantically interoperable, "open" technologies ready for bundling in COTS products. As the public network infrastructure becomes more secure and interoperable, the military can wean itself away from its use of private stovepipe networks for the bulk of its cyber activity. It can reserve private classified networks for truly specialized, protected, non-network-centric activity.

Finally, as the quintessential business management expert, Peter Drucker, said, "You get what you measure and reward." The US Defense Community currently measures

---

[30] This use (and prior) is a much stronger meaning of semantic interoperability that usually meant. Usually, it's just supplying bits that are understood as intended.

and rewards paperwork and enormity of stovepipe programs – both of which are at odds with the agility required for success at NCW [31] [32]. If it hopes to field network-centric capability superior to its adversaries, the US Defense Community must begin to measure and reward demonstrated acquisition agility, *i.e.* speed-to-capability[33]. Happily, another lesson learned in the 21st Century is that meteoric success is possible for those willing to eschew sunk cost arguments and boldly embrace the art-of-the-possible in an Information Age.

---

[31] GAO. (2009). *Charting a Course for Lasting Reform.* Washington: GAO. and DoD. (2008). DoD. (2008). This GAO report describes how the size of DoD acquisitons across the board have grown massively -- to their detriment -- over recent years.

[32] DoD. (2008). Actions Requred to Comply With Subtitle III/CCA . *DoD Instruction 5000.02* , Encl 5; Table 8; p48. This table correlates 11 policis required for Clinger-Cohen Act (CCA) compliance to mandatory documents to describe, requirements definition, analysis of alternatives, specifications, IA compliance, etc. Many policy elements require several supporting documents. Each serially completed document is long, expensive, and takes months to prepare. This documentation is redundant across many similar programs and systems. Paradoxically, the intent of CCA intent is to streamline government acquisition by adopting commercial best practice.

[33] Gunderson, C. R. (2009, May 5). Memoradum for the Record re Value-Based Evolutionary Framework.