Communications Technology Trends:

Implications for the Defense Industry and its Clients

Steven Shepard
Shepard Communications Group, LLC
+1-802-878-0486 (Office)
+1-802-238-1007 (Mobile)
+1-802-872-9587 (Fax)
Steve@ShepardComm.com

Executive Summary

There is a change underway in the Defense Industry, brought about by an evolution in the Department of Defense's (DoD) perspective on effective warfare, a realization on the parts of both the DoD and its suppliers of the remarkable role that network and information management technologies can play in warfare scenarios, and economic forces that press the need for more cost-effective solutions to challenges that tend to be highly capital-intensive and that rely on enormous volumes of human capital as well.

This evolution heralds a sea change for the Defense Industry, a move from dependence on a small number of large, multiyear contracts to larger numbers of smaller, short-term contracts, as well as a distributed architecture model that effectively separates "the shooter" from "the weapon."

As revolutionary as this transformation may be for the Defense Industry, it is not new to the public sector. The changes that are just now being felt in the Defense sector have been underway in the more traditional enterprise sector for nearly 20 years. And while they have presented organizational, technological, human capital, and financial challenges, the companies that have gone through them have emerged more competitive and capable than they were before.

A re-education of sorts will be required within the Defense Industry to mentally retool for the transformation from a centralized model to a more distributed one. This shift, which is as much philosophical as it is technological, must occur soon. Companies that undertake the shift early on will be early winners in the game.

"In its ultimate form, the entire theater of operations will be networked. Sensors will reside on every piece of equipment and every person populating the field of operations, and information collected by those sensors will be processed in real time using artificial intelligence support to prioritize threats and challenges. In-charge personnel will be able to choose from a portfolio of response options to identify and select targets.

"As a result, the time between sensing, processing, deciding and acting will fall dramatically, allowing forces to target the opposition before they can respond."

-- Retail executive describing the company's RFID initiative.

Part One: The Enterprise Transformation

Since the early 1980s, the typical American enterprise has undergone a reinvention process. This process has changed their overall business philosophy, changed how they think about customers and competitors, even changed the nature of the products and services they sell.

The first major shift was an evolution away from the vertically integrated, full-service corporation toward a flatter, more specialized organization that relies on relationships with contractors and third party vendors to deliver a complete solution to their customers. This came about because of a changing competitive model, globalization, and the inability to operate as a "soup-to-nuts" operation in the face of changing regulatory, legislative and competitive forces.

The second major shift, and one that follows logically on the tail of the first, is a reduced dependence on hard products and a greater dependence on information and knowledge-based products. Corporations have come to realize that the data contained in their enterprise databases can be mined and converted to useful information, which can in turn be converted to knowledge about customer behaviors – a powerful competitive advantage. As technology-dependent analysis tools such as software-based data mining, information management, knowledge management, customer relationship management (CRM), and enterprise resource planning (ERP) have matured and found themselves in demand, and as storage technologies such as storage area networks (SANs) and storage access interfaces such as Fibre Channel and Gigabit Ethernet have emerged, corporations have begun to take advantage of this resource. The result is better competitive positioning, stronger sales, and faster response capability to marketplace demand shifts.

The third big shift is the evolution from a hierarchical, top-down management regime to a distributed model that moves decision-making to its lowest logical place in the managerial hierarchy. The result is a tighter relationship with the customer and faster, more accurate service provisioning.

Art, Plato once observed, is a meticulous imitation of life. In the same sense, network architectures *always* mimic the architectures of the corporations that they serve. In the 1970s, when companies were entirely hierarchical and decision-making occurred at the top of the pyramid and then filtered downward, mainframe-centric computing was the norm. IBM's Systems Network Architecture (SNA) was exemplary of this model: All computing (decision-making) occurred in the mainframe (top of the pyramid) while the so-called "dumb terminals" (employees) were given what they needed to know to get the job done.

> A greater vulnerability than legacy assets is a legacy mindset. It may be easy to grasp this point intellectually, but it is profoundly difficult to practice. Managers must put aside the presuppositions of the old competitive world and compete according to totally new rules of engagement. They must make decisions at a different speed, long before the numbers are in place and the plans formalized. They must acquire totally new technical and entrepreneurial skills, quite different from what made their organizations (and them personally) so successful. They must manage for maximal opportunity, not minimum risk. They must devolve decision-making, install different reward structures, and perhaps even devise different ownership structures. They have little choice. If they don't deconstruct their own businesses, somebody else will do it to them.
>
> -- P. Evans and T. Wurster, *Blown to Bits*

As time passed and corporations evolved, a flattening occurred as Apple, HP and Xerox arrived with their concept of distributed management. Soon thereafter came the Local Area Network (LAN) and the PC, a pair of innovations that ultimately facilitated the arrival of distributed desktop computing. As corporations became more distributed, so too did network and computing resources.

Technology Directions

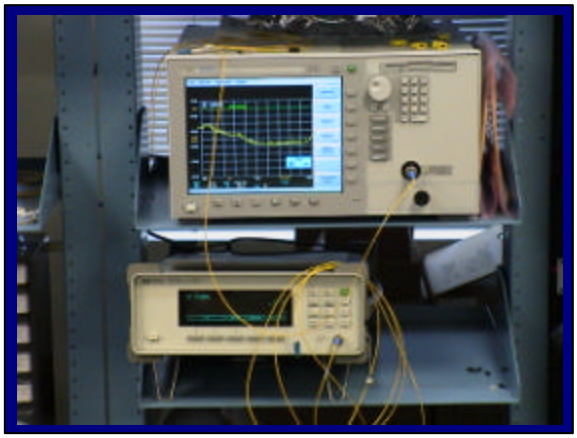
A collection of technology areas have emerged that are redefining the way computing resources and the networks that interconnect them provide services to the Defense Industry. They are the same technologies that are re-orienting the enterprise environment, albeit with different objectives. These technologies, and their implications for the Defense Industry, are described in detail below.

The Packet Evolution

The ongoing convergence of technologies, services and companies to create multiservice networks is made possible by the continuing development of network-based applications that rely on the TCP/IP protocol suite for addressing, traffic management, and transmission quality. TCP/IP was initially created to serve best-effort network environments, but over the years it has been called upon to do much more than that. First, bandwidth and storage have become extremely affordable and large quantities of both are for the most part universally available. Second, networks are being used for more than dial tone – they transport voice, video, data, still images, audio, and a host of other traffic types, each with proper levels of delivery quality. Third, network implementers (particularly those who own the IT budget) have long clamored for a converged network that allows them to reduce the capital intensity of their managed networks and the attendant operational costs associated with them. Finally, the issue of quality of service (QoS) over packet networks has been resolved in three ways: (1) the enterprise owns the end-to-end network and therefore has the ability to establish usage policy that results in a network environment with managed QoS; (2) there is an underlying switching layer (ATM, for example) that establishes a high-quality point-to-point path over which IP packets are transmitted; or (3) the network

relies on some form of QoS protocol like Multiprotocol Label Switching (MPLS) that can overcome the shortcomings of IP from a QoS perspective. Whatever the case, IP has now entered the big leagues and IP can now offer carrier-class voice – as well as a plethora of other services, all over a single converged network infrastructure. Packet, then, unquestionably lies at the heart of the future network. Does this spell the demise of traditional circuit switching? Not in the near term; circuit-switched voice provides the highest service quality, but at a cost. Over time its use will diminish. Meanwhile, IP-based infrastructures will continue to evolve, and will find increasingly important roles in the Defense Industry.

Optical Networking



Optical networking continues to play a major role in the evolving network, in spite of all claims to the contrary voiced in the trade rags. Yes, there is a substantial oversupply of transport capacity, but even during the "dark period" (2000-2002), network traffic continued to grow, and continues to grow *now* - consuming much of the bandwidth glut. Furthermore, while there is still far too much bandwidth deployed between the so-called Tier One cities (Dallas to Houston, or San Francisco to LA, for example), there is a measurable dearth of it between Tier Two and Three cities. Their demands will grow and optical transport will be the solution. Furthermore, expanding usage of multimedia, wireless gaming, videoconferencing and other bandwidth-intensive applications will spur the need for additional fiber. Additionally, metro areas will continue to grow and will have an ongoing need for high-bandwidth transport. Technology solutions such as switched Gigabit Ethernet (GbE) are emerging as cost-effective alternatives that take advantage of optical infrastructure, further consuming the glut of transport capacity. Naturally, the Defense Industry's increasing reliance on information technology and the need to transport larger and larger multimedia files across the globe will drive demand for optical transport in that space.

Broadband's Arrival

Applications today are fundamentally dependent upon the availability of low-cost, universal broadband access and transport solutions, and service providers are counting on being able to deliver multiservice solutions over a single network that uses bandwidth-on-demand to make good on the promise of services on demand. Whether the bandwidth is delivered via DSL, cable modem or a wireless interface is immaterial. What matters is its availability and ubiquity for the support of on-demand computing, content access and communications.

Wireless broadband has recently garnered a great deal of attention and will play a significant role in the evolution to network-centric warfare. Technologies such as 802.11 (the various flavors of Wi-Fi), 802.16 (Wi-MAX), and 802.15.4, in concert with scattered sensor arrays, will provide universal, real-time connectivity in the field of operations and will allow battlefield commanders to manage disparate resources from any location. Wireless is discussed in greater detail, below.

Wireless

Wireless is changing faster than any other technology area today, and for good reason. It has a large percentage of the industry's R&D resources focused on it, promises wonderful things that can be tangibly appreciated, requires minimal infrastructure capital, and is accessible (and therefore visible) to the average person. The long awaited 3G wireless is approaching, and while it is in a state of unbridled chaos at the moment it *will* settle down and deliver on its promises.

Wireless device manufacturers like Samsung, Nokia, Sony, Motorola, Kyocera, and a host of others are gradually releasing devices onto the market that incorporate clusters of functions that users say they want in a single device: phone, PDA, PC for Web surfing, GPS, universal remote control, memory card slots, 802.11, Bluetooth, speakerphone, MP3 player, voice recorder, and a battery that lasts long enough to use them all. 802.11 (Wi-Fi) has taken the world by storm and is fast becoming the preferred connectivity solution for local area networks because of its simplicity (no wires) and bandwidth. And a number of new technologies that are currently looming on the horizon, 802.16 (WiMax) and 802.20 (mobile broadband) will provide even more flexible options. 802.16 promises connection speeds between ten and 100 Mbps over service radii as wide as 30 miles, while 802.20 is lower bandwidth (1 Mbps) but will work for users traveling at high speed, such as in a European commuter train moving at 100 mph. Pay attention to these technologies: When they hit they will leave a very large dent.

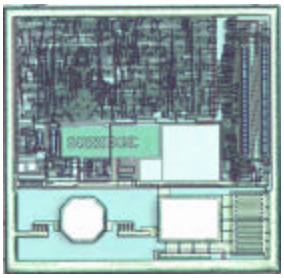
RFID and Sensor Technologies

Much of the content that will travel across wired and wireless broadband networks will be collected by passive and active sensor arrays deployed strategically throughout the theater of operations. The sensor technology enjoying the greatest interest today is RFID, a technology that relies on passive low cost sensor chips, no larger than a pinhead, that can be affixed to essentially anything (even woven into clothing).

Passive RFID tags are not powered internally; instead they rely on the reader to supply whatever power they require to operate. As a result, they are lighter, less expensive, and smaller than active RFID tags, and have essentially unlimited lifespans. Their only downside is a shorter read range and the need for a higher-powered reader.

Passive tags are pre-programmed and cannot be modified. Their most common application is as a "digital barcode," used to track the location and usage of products. Military applications include ordinance and supply inventory tracking, personnel monitoring, and vehicle fleet management.

Active RFID tags are larger than their passive counterparts because they are powered by an internal battery and can be rewritten or modified. An active RFID tag's memory size varies according to the intended application and can incorporate as much as a megabyte of storage. In a typical active RFID system, the tag might give an automated weapon a set of instructions, and the weapon would then report its performance to the tag. This encoded data would then become part of the device's history, or could be transmitted back to a central location for device management. Because active tags have internal batteries, they typically have greater distance capabilities than passive tags. They are also bigger, more expensive and have limited lifespans.



RFID technology (an example of which is shown at right) holds great promise in the field of network-centric warfare and will work closely with sensor-aware networks. Imagine a situation where thousands of passive RFID sensors the size of a pinhead are dispersed across a field of battle like fertilizer on a lawn (sometimes known as *Smart Dust*), instantaneously creating a universally networked environment that can track troop movements, vehicle location, supply consumption, ordinance accuracy and availability, and a host of other data sets.

Network Management

Network management (the process of managing the network in its entirety as a multifunctional organism) and element management (the process of managing the individual elements that make up the network) have been viewed as one and the same for far too long. Most manufacturers offer very good element management systems with their products; far fewer companies offer an integrated network management system that views all the elements as a consolidated whole and helps the service provider deliver seamless service. Fewer still offer systems that facilitate predictive management, or

that look have the ability to look outward toward the user as effectively as they look inward toward the network. In the same way that companies like Amazon and Dell engage in data mining processes to anticipate user demand for products on a customer-by-customer basis, network management software must evolve to provide a service-matching bridge between the user and the network itself. In the Defense Industry, this becomes crucially important as the volume of data being transported across the network increases.

Watch the Unexpected Players

In the classic role-play game Dungeons and Dragons, one character that occasionally pops up unexpectedly as the result of a roll of the dice is called a "Berserker." Berserkers have no function other than to inject chaos into the game – sometimes good, sometimes bad, but *always* unpredictable. The technology industry is quietly being surrounded by an army of Berserkers that are in the process of redefining the roles of networks, computers and the applications that they serve. They are also irreversibly changing the relationship between end-users, services providers, and manufacturers.

In the Defense Industry, these berserkers include such firms as Microsoft, HP, IBM, EMC^2, and many others. Suppliers to the industry should pay particularly close attention to the marketplace as the influence of these new arrivals is felt. In keeping with the evolution from single large DoD contracts to multiple smaller agreements, these firms will introduce significant confusion as they find seats at the table.

Scene Shift: The Defense Industry

The same model of network-centric computing is now appearing in the defense environment in the form of *Network-Centric Warfare (NCW).* The vision of NCW is a compelling one: reduce battlefield mass by replacing manned weapons with remotely operated devices equipped with an exhaustive array of sensors that allow them to identify potential targets, determine its threat posture, target it precisely, and fire economically. The sensor array is interconnected via a high-speed wired or wireless (or both) network that delivers the raw "sensed data" to a sophisticated data mining application that converts it to tactically useful information. The information is then delivered to strategic decision-makers who analyze the information, converting it in the process to knowledge upon which they can now make informed decisions. These decision-makers may be in the theater of operations, but are most likely far away.

A good example is the Joint Direct Attack Munitions (JDAM) model, a combination of a weapon (a bomb) and a sensor (GPS). Similarly, the Predator and the Global Hawk remotely operated vehicles provide data gathering and transport without the need to place a warfighter in harm's way.

In summary, then, network-centric warfare has evolved and taken root in the same way that network-centric computing has evolved, as shown in the table (below). But what are the key design elements in the NCW transformation?

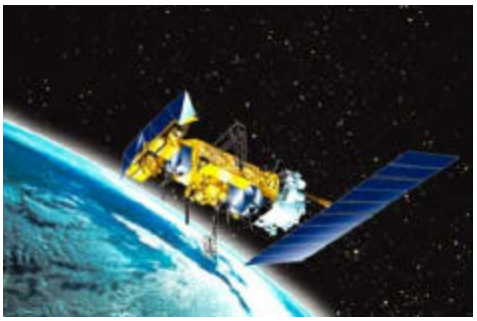
Information Technology: Mainframe-Centric	→ Distributed Computing
Business Dynamics: Corporate-Centric	→ Virtual Corporation
Warfare Dynamics: Platform-Centric	→ Network-Centric

Change Elements

There are four major change elements involved in the shift to network-centric warfare: the overall functional transformation, the rise of NCW itself, the creation of distributed, joint operations, and the evolving role of the defense contractor.

Transformation

Transformation defines the resource shift that is integral to the overall change. It includes the application of command and control software, communications facilities, and systems technologies to improve the efficiency, accuracy and responsiveness of battlefield assets.



Network-Centric Warfare

Network-Centric Warfare (NCW) defines the process of equipping all weapons, weapons components, vehicles, personnel, and ancillary infrastructure components with sensors and real-time processing capacity, which together can prioritize threats and intelligently select targets. It is the linkage of sensors, decision-makers, and combatants over a high-speed, standards-based, survivable network.

Joint Operations

In addition to the business of defensive warfare, operations related to intelligence gathering and homeland security will cause a change in both the applications required to carry them out and the interdisciplinary operations necessary to make them execute effectively. The elimination of "silo operations" will be a large part of this evolution; so too will the one-to-one relationships that currently exist between defense contractors and individual DoD agencies.

The only thing harder than getting a new idea into the military is getting an old one out.

-Liddell Hart

The Evolving Role of the Defense Contractor

Perhaps the greatest change will occur for the defense contractor. Instead of serving exclusively as a manufacturer and provider of weapons systems, the contractor will become a "prime contractor" for systems design and development and will serve as a key, trusted advisor to the DoD. This is a necessary, complex and (ultimately) inordinately valuable shift for both the service provider (defense contractor) and the customer (DoD).

The Challenges

The value of a meshed network increases as a function of the square of the number of nodes in the mesh. –Metcalfe's Law

No node can be worth more than the connectivity it provides.

--Barnett's Conundrum

Network-centric warfare represents a significant architectural, philosophical, and managerial shift, illustrated nicely by Liddell Hart's quote at right. This evolution, from an environment in which the sensor and the shooter are one and the same, to a model in which the sensor is distributed across the field of operations and the shooter may or may not be a human, is immensely complex, operationally challenging, philosophically difficult to accept, but absolutely necessary. If the goal of the DoD is to reduce headcount in the battlefield while at the same time improving the effectiveness and accuracy of deployed weapons systems, a knowledge and capability matrix must be adopted as part of the functional model. This matrix relies on the capabilities of diverse human intelligence sources scattered throughout the military; their combined knowledge and capabilities bring about the vision of Metcalfe's Law, which

observes that the value of a network increases exponentially as new nodes are added. Lou Platt, the former CEO of Hewlett Packard, once observed that "If HP knew what HP knows, we'd be three times more profitable." The same is true for the Defense Industry: the strategic management and deployment of knowledge resources yields significant capability multipliers. Ironically, when applied to a battlefield scenario, the ability to accelerate the process of sensing, processing and taking action allows theater commanders to slow down their response – thus avoiding friendly fire accidents and improving the effective response against known, real targets of opportunity. And if done correctly, this shift brings about a sweeping and necessary managerial change. Command-and-control hierarchies are modified, the decision-making process accelerates, relationships between coalition forces evolve, and the role of suppliers evolves. Data, information and knowledge replace "battlefield mass," resulting in a level of awareness that is unprecedented and which can be administered remotely just as effectively as if it were done locally.

NCW Challenges

Of course, this evolution is not without challenges. NCW is still in the relatively early stages of evolution and therefore requires significant research and development (R&D) dollars. This can cause economic pain for suppliers accustomed to offering established, mature solutions to DoD projects; these firms must reallocate budgets to ensure an balance between maintenance projects and those that require R&D investment.

The best way to predict the future is to invent it.
--Alan Kay

A second challenge is one of pushback: As often happens with new technologies, the DoD is placing a great deal of emphasis on technologies that are unproven and only minimally tested – but that they perceive to hold promise for the future. As a result there is significant ambiguity over the intended choice of platform direction and therefore the technologies required to support it.

Alan Kay, the inventor of the laptop computer, once observed, "the best way to predict the future is to invent it." He's right, and his quote is particularly appropriate with regard to the development of NCW. Technology and infrastructure providers must reorient themselves to become "future creators," working closely with their DoD counterparts as trusted, strategic advisors to guide them toward a more certain future.

Drafting the Future

As contractors position themselves to offer enhanced services along the value chain between themselves and the customer, four goals emerge as critical success factors. These goals must be addressed if (1) NCW is to become real and (2) the role of the defense contractor shifts toward an enhanced services role. The goals are:

If you don't know where you're going, any road will take you there.
-- Alice, in Wonderland.

- *Reduce interoperability gaps between armed forces agencies and the contractors that support them.* The military, like most large bureaucratic organizations, is administratively compartmentalized into functional "silos" that operate in a largely autonomous fashion. By combining the capabilities of these disparate organizations and taking advantages that Metcalfe's Law promises, a far more efficient and effective macro-organization can be crafted.
- *Create and disseminate a shared vision for the NCW model.* The key to successful implementation of *any* major organizational shift such as NCW is the early creation and dissemination of a common clear vision of the intent of the changes that will be brought about by the shift. Every organization in every sector of the industry must understand the common goal. Without a shared vision of the direction and objective that the organization seeks, success will be difficult.

- *Reduce linkages between individual contractors and military verticals.* For reasons that have largely been lost in the mists of time, strong business relationships have evolved between certain defense contractors and specific vertical organizations in the military. As the business model changes and calls for multiple smaller contracts instead of single large agreements, this one-to-one model will no longer be as effective or lucrative as should be. Defense contractors will be called upon to serve as "prime contractors" on large projects, assembling virtual teams to deliver complete solutions.
- *Provide consultative support and a shift in focus from hardware to software systems by contractors.* In the same way that the evolution to network-centric computing involved a renewed focus on software control, network-centric warfare requires a similar retooling effort to recognize that the forced separation of sensor and weapon requires software control.

These four goals will result in the achievement of a number of key DoD objectives: reduction in the overall cost of military operations; reduction in the number of both military and civilian casualties; and an improved ability to adapt to changing threat postures in real-time. These goals, in turn, support the six key objectives of the DoD: protection of both domestic and overseas forces; sustained power and shows of force in all active theatres of operation; denied sanctuary for the enemy; protection of the increasingly important American information network; functionally meshed armed forces organizations; and the sustained ability to maintain access to space and protect space-based assets.

In summary, then, business and military operations rely on similar technology infrastructures, shown in the table, below.

Business	Military
Circuit-to-packet	Packet-based global grid
Optical and broadband	High-speed wired and wireless networks
Sensors (RFID)	Grid-connected sensors
Mobility and ubiquity	Secure wireless
Component shifts	Reduced "electronic real estate"
Role of the Berserkers	Changing role of contractors
Network management	Command grid
Enterprise software applications	Network-centric warfare

How, then, does this technology shift and the introduction of a plethora of new computing and network technologies fit into the concept of the military's global command grid? That's the subject of the next section.

Part Two: Putting the Technology to Work

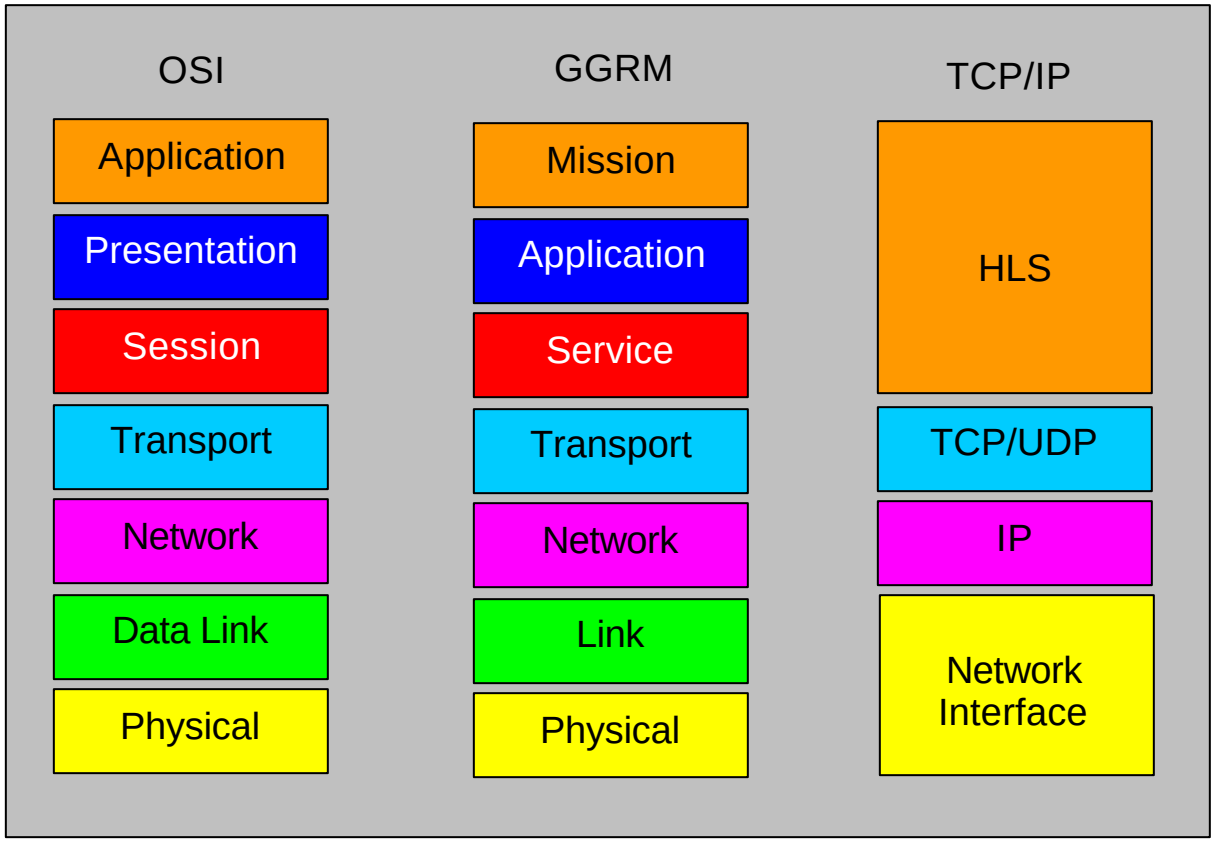
In this second section we introduce the concept of layered architectures, a central component of network-centric warfare. As the illustration (below) shows, the process of transmitting information from one machine to another can be divided into a collection of functional layers.

Data communications networks are often described in terms of their architectures, as are protocols. Protocol architectures are often said to be *layered* because they are carefully divided into related but non-overlapping functions. This "division of labor" makes the deployment of complex networks far easier.

Perhaps the best-known "family" of protocols is the International Organization for Standardization's Open Systems Interconnection Reference Model, usually called the OSI Model for short. The seven-layer OSI Model provides a logical

way to study and understand data communications and is based on the following simple rules. First, each of the seven layers must perform a clearly-defined set of responsibilities which are unique to that layer, to guarantee the requirement of functional modularity. Second, each layer depends upon the services of the layers above and below to do its own job, as we would expect, given the modular nature of the model. Third, the layers have no idea how the layers around them do what they do; they simply know that they do it. This is called transparency. Finally, there is nothing magic about the number seven. If the industry should decide that an eighth layer is needed on the model, or that layer five is redundant, then the model will be changed. The key is functionality.

It is important to understand that the OSI Model is nothing more than a conceptual way of thinking about data communications. It isn't hardware; it isn't software. It merely simplifies and groups the processes of data transmission so that they can be easily understood and manipulated.



Each layer builds on the work performed by the layers that surround it, and each layer has a specific set of responsibilities.

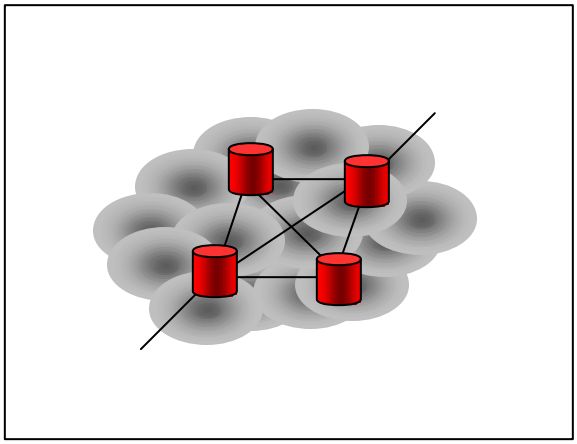
The *Application Layer* offers a set of specific services to the application itself (e-mail, for example) and is concerned with the meaning or semantic content of the message. Services offered at layer seven include SMTP, X.400, HTTP, FTP, etc.

The *Presentation Layer* worries about the form or syntax of the message being transmitted. It cover such functions as compression, encryption, and code conversion. It offers a set of general services that can be used by any application.

The *Session Layer* is concerned with establishing a logical relationship between the sender and the receiver. For example, many computer systems (think about AOL, for example) have a single host array that conducts simultaneous sessions with hundreds of thousands of users. The Session Layer is responsible for ensuring that the information carried in each logical session *stays* in that session.

The *Transport Layer* is responsible for end-to-end, message-oriented delivery. In other words, it operates at the message level – it doesn't care about bits, or frames, or cells, or packets. To do this, it receives the message from the layers above it, divides it into packets, numbers the packets, and hands them to the network layer, which routes them according to its own whims. At the receive end of the circuit, the transport layer reassembles the incoming numbered packets into a complete message.

The *Network Layer* is responsible for message or packet routing and congestion control. Instead of managing on a point-to-point basis, it manages across the network, selecting the best route based on known congestion conditions, facility problems, cost, or distance. The Network Layer concerns itself with packets.



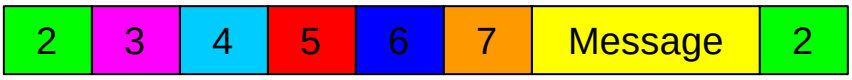
The *Data Link Layer* is responsible for bit-level error detection (and sometimes correction), data framing, and link control. It is responsible for managing the series of point-to-point connections between an array of switches that make up a typical network, as shown in the illustration at left. The switches, shown as red cylinders, are interconnected via a collection of circuits that can be connected end-to-end to create a facility from one end of the network to the other. This is, in fact, the responsibility of the switches. The Data Link Layer is concerned with frames of data, or in some cases (ATM, for example), cells.

Finally, the *Physical Layer* defines the physical interface over which the data is transmitted, including connector pin configurations, voltage levels, optical transmission parameters, channel assignments, and so on. It concerns itself with the health and welfare of the individual bits that make up the message.

When a message is created by an application for transmission, it is first handed to the Application Layer, which recognizes the nature of the message (an email message, for example), converts it to a standard format for email transmission (SMTP or X.400), and appends a header that identifies the message as e-mail, so that the operating system at the receiving computer can direct the message to the appropriate application. It then passes the message to the Presentation Layer, which (if required) encrypts and compresses it, adding the appropriate header. It then passes the growing message to the Session Layer, which adds its own logical session identifier as yet another header before passing the message on to the Transport Layer.

The Transport Layer chops the message into a series of packets that it numbers (another header) before handing them down to the Network Layer, which addresses each packet (header) before handing them down to the Data Link Layer. The Data Link Layer receives each packet, builds a frame (header AND trailer) around it that includes the address of the next switch in the chain along with some bit-level error control data, then hands each packet down to the Physical Layer, which transmits them as a series of bits across the selected facility. At the receiving machine the process is reversed; as the information moves up the stack, each layer interprets the header from its corresponding layer at the originating end before removing it. Ultimately, all the headers added during the transmission process are removed, leaving the native

message, which is finally handed to the receiving application. This is illustrated by the graphic, below; the numbered header/trailer components are added and removed as required by the transmitting and receiving entities.



Of course, OSI is not the only "protocol game in town." One of the better-known alternative protocol stacks is the TCP/IP stack which governs the inner workings of the Internet. In TCP/IP, the Physical and Data Link Layers are combined to form the Network Interface Layer. The Network Layer is left alone in the form of the Internet Protocol (IP), while layer four, the Transport Layer, comprises two key protocols, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP is an ironclad, guaranteed delivery service protocol, while UDP offers best effort service. Needless to say, TCP requires significantly more overhead than UDP since it has more to do. Finally, the Higher Layer Services comprise the functions of OSI's layers five through seven.

Defense Applications of OSI

OSI is clearly far more complex than this mercifully short explanation can reveal. However, the OSI Model construct does a very good job of segmenting the complex task of data transmission so that networks can be designed around the individual components of the transmission function. And while OSI itself has little practical application for defense applications, the layered model has enormous implications, because the military has chosen a layered model known as the *Global Grid Reference Model (GGRM)* as its overall architecture for building network-centric warfare technologies.

Like OSI, the GGRM is a seven-layer model that describes the complex process of moving data through a military network that controls a NCW environment. As the comparative table (above) shows, the lower four layers are identical to OSI, providing the same set of services to the upper layers that the lower four OSI layers provide. At layer five, however, things begin to change. Instead of a Session Layer, the GGRM has the *Service Layer*, which does many of the same things that the Session Layer does. It supports a number of applications that are not accessible to the user: rather, they are used by the underlying operating system of the computing devices at each end and by the network operating system (NOS) to ensure logical connectivity between communicating processes. Examples include network address translation, domain name management, etc.

Just above the Service Layer is the *Application Layer*. The Application Layer is accessible by the user and offers a set of common mission-specific applications that support the *Mission Layer* above it, including network management and transport security.

The Mission Layer supports unique military applications that may vary from theater to theater. For example, network support requirements of remote unmanned observation platforms are different from those of a forward manned command post that performs analysis of data collected by sensor arrays.

One observation that must be made: Some agencies believe that the global grid supported by the GGRM comprises only the lower four layers of the GGRM; others believe it incorporates all seven layers. The argument is largely semantic. Like OSI, the lower four layers tend to define the network itself, while the upper layers define the logical relationship between the physical network, the applications, and the logical interdependencies that must exist between them.

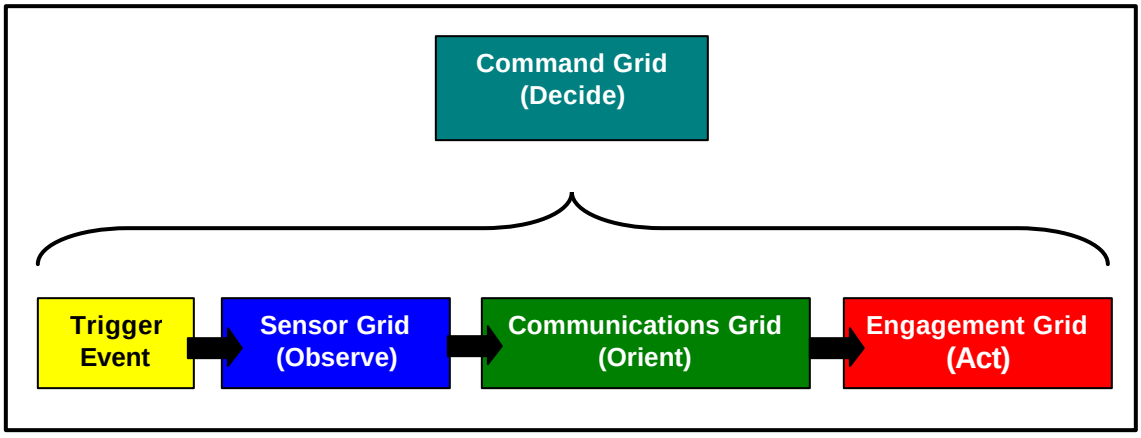
The GGRM in Action

John Boyd, a 1950s fighter pilot, conceived the concept of Boyd's Loop as a way to gain tactical advantage over an adversary by taking advantage of their own weaknesses. The loop, shown below, consists of five components. First there

is some kind of triggering event that causes the loop to engage. For example, a threat detection system comes online and notifies. Next, there is an observation component that is used to collect the data about the threat for analysis. Third, an orientation stage is used to correlate the data. Fourth, a decision process mechanism analyzes the collected data, turning it into useful information, and once that has been accomplished the action stage kicks in, taking whatever action is required based on the information at hand.

Under the terms of network-centric warfare, Boyd's Loop is equally applicable. A triggering event causes a collection of sensors (sensor grid) to identify an event that demands a potential response. The sensors transmit their uncorrelated data over a high-speed communications network (communications grid) to a command function(command grid) that analyzes the data before passing it to an engagement grid which activates a weapon or otherwise correlates a proper response to the threat.

This O-O-D-A model continues to have value in the modern military – in fact, it has even greater value than ever before, because the ability to deliver a reasonable response to a threat using remote sensing technologies on a battlefield with limited engaged personnel is a compelling and powerful argument. As noted earlier, the ability to accelerate the analysis of a threat posture permits a deceleration of the response until a proper response can be calculated, thus reducing the potential for collateral damage and friendly fire accidents.



In Conclusion

It is an inevitable fact that the technological advancement of modern warfare parallels that of modern business. Speed of development and flexibility are key characteristics; data, information and knowledge are the principal drivers of technology and application development. The customer, in this case the DoD, needs both strategic and tactical guidance from its suppliers in the form of knowledge management and enhancement, in addition to delivery of hard products. Today, defense contractors find themselves bidding on small numbers of relatively large contracts because the centralized nature of the military complex lends itself to the development of monolithic command control systems that interoperate with weapons systems. As network-centric warfare develops and command and control infrastructures become more distributed, and as the concept of distributed sensor-controlled weapons systems become the norm for a new breed of software-controlled weapon, contract opportunities will also become more distributed, evolving to a model of multiple smaller contracts being bid on by a wider array of specialized competitors. Whereas General Dynamics, Boeing, Lockheed Martin and Grumman compete today for large lucrative contracts, in the future they will find themselves competing against the likes of Microsoft, SAIC and Computer Associates, to name a few. As an indicator of the critical nature of this relationship, General Dynamics acquired Veridian for $1.5 billion, while Lockheed acquired Titan for $2.4 million. It is critical, therefore, that defense contractors like General Dynamics focus on differentiation characteristics. Recognizing the

shift toward a network-centric demand model is the first critical stage of this refocusing effort. The second is a fundamental retooling of the basic deliverable, which is not as major a step as it sounds. The company is already beginning to take the first necessary steps, but the effort must continue.

General Recommendations

Defense contractors must make a strong commitment to the early stage R&D effort that is required to move into the early phases of network-centric warfare. They must continue to acquire consultative capability in the areas of software systems design, wired and wireless sensors, and signaling systems. They must do this while engaging in targeted discussions with the DoD designed to position them as a consultative, strategic-level business partner, designing systems and applications based on the four-grid model described earlier. This model is widely understood and is applicable in the enterprise world as much as it is in military scenarios. It is critical, therefore, that contractors pay particularly close attention to technologies that are being deployed in the enterprise space, because those technologies typically lead the military by several years. By recognizing and responding appropriately to the shift from mainframe-centric computing to a distributed model, as well as on the shift from a platform-based model in which the shooter and the sensor are one and the same, to a model in which the two are separate and distinct, defense contractors can demonstrate that they are highly differentiated and favorably disposed to applying themselves to the NCW research and development effort that leads to product contract assignment.

C4IST:

Command, Control, Computers, Communications, Intelligence, Surveillance, and Targeting.

Defense Industry Recommendations

As far as the Defense Industry is concerned, there are several actions that should be undertaken. First, the organization's compelling engineering and design capabilities make it an ideal partner for smaller companies with solid products that are looking for a conduit to the market. The trust that the market places in the Defense Industry is a powerful tool that can be used to create professional relationships with these companies, broadening the organization's presence and capability set.

Second, the Defense Industry should strive to climb the "GGRM food chain." The organization already operates reasonably well at the lower layers, but true differentiation occurs at the higher layers, specifically at the mission and application layers. Please understand: this movement upward does not imply an abandonment of the lower layers and the products that reside there; what it *does* imply is a move toward integration of the entire model, from Physical (Layer One) through Mission (Layer Seven), creating a whole new family of product capabilities. For example, the combination of the firepower of Lethality Systems, the sensing capabilities of Detection Systems, and an as yet undefined data analysis scheme will result in enhanced products that span the entire range of capabilities described in the GGRM. These products will in turn provide the mechanism for reduced battlefield mass, discrete targeting capability, and lowered overall deployment cost.

Critical topics that must be addressed include but are not limited to:

- The concept of network-centric warfare
- The OSI Model and layered protocol concepts
- TCP/IP as an alternative to OSI and its role in IP-based networking
- GGRM
- RFID and other sensor solutions and applications

- 802.11, 802.16, 802.15.4 and other wireless technologies
- Components and their role in NCW (semiconductors and optoelectronics)
- Network Management and its role in NCW command and control infrastructures
- MPLS as a QoS alternative
- QoS and its relative importance in military network applications
- Optical Networking
- Gigabit Ethernet as an evolving, low-cost access and transport technology
- Enterprise applications that lend themselves to military scenarios such as data mining, information and knowledge management, customer relationship management, supply chain management, and enterprise resource management

As the role of the defense engineer broadens, it is critical that they understand the changing role of data collection points (the sensor grid), the network (the communication grid), the analysis applications it interconnects (the command grid), and the decision management tools that control field resources (the engagement grid). This is the promise of NCW; it heralds major opportunities for defense contractors that understand the inexorable, distributed evolution that is underway.

Steven Shepard is the president and founder of the Shepard Communications Group, a Vermont-based firm that provides industry analysis, technical education, management consulting, and media development to technology companies throughout the world. He can be reached at +1-802-878-0486, or via e-mail at Steve@ShepardComm.com.