REALIZING THE NETWORK-CENTRIC WARFARE VISION: NETWORK TECHNOLOGY CHALLENGES AND GUIDELINES

Dr. James A. Freebersyser
Advanced Technology Office
Defense Advanced Research Projects Agency

Joseph P. Macker
Information Technology Division
Naval Research Laboratory

ABSTRACT

An expanded and improved information technology capability is the fundamental heart of the network-centric warfare (NCW) vision. The NCW vision is worthy and is a direct path to achieving improved collaborative power and information dominance. The potential benefits of diverse information sharing and interconnection are manifold, but at the same time difficult to fully predict and quantify. Moreover, along with unforeseen benefits, additional concerns often arise with technological enhancements to information sharing and access. In this paper, we consider several sources of 'friction' working against achieving the NCW vision, we outline the technical challenges that must be met to overcome this friction, and we make some suggestions in progressing towards a set of solutions.

BACKGROUND

In *Joint Vision 2010* the Joint Chiefs of Staff outline an operational concept that builds heavily on various information-age technology advances. Information technology systems are described as providing the "capability to collect, process, and distribute relevant data to thousands of locations," thus allowing our forces to gain "dominant battlespace awareness." Individual warfighters are described as having "an array of detection, targeting, and communications equipment." This worthy and ambitious vision for future military networks is further extended by the stated desire for "greater mobility and increased dispersion" of our forces. As stated in *Joint Vision 2010*, our forces "must have the ability to outpace and outmaneuver the enemy." As shown in Figure 1, the notion of network-centric warfare (NCW) implies the ability to exchange information between network nodes participating in the information, sensor, and engagement grids as required by mission needs [CG98].

Across the information grid, network centric warfare deals with a varied heterogeneous set of mission environments, applications, and subsystems. Figure 2 shows an emerging taxonomy of network-centric warfare architecture and related broad performance parameters [CG98]. Weapons control, force control, and force coordination are clearly identified as having different requirements and varied primary content support needs.

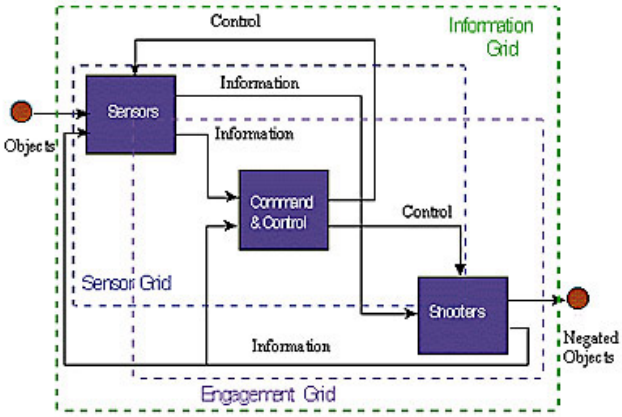

Figure 1: Information grid encompasses both sensor and engagement grids.[CG98]

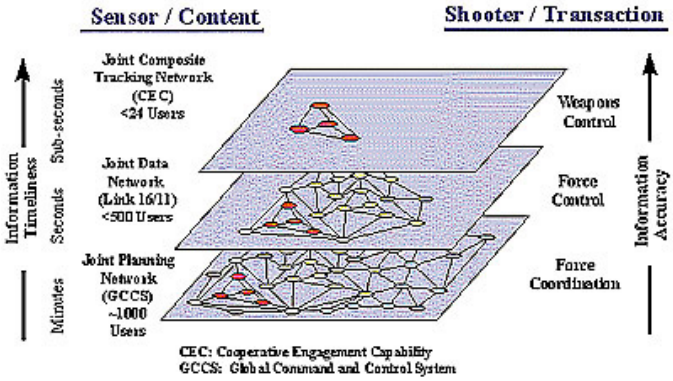

Figure 2: Emerging Network Centric Warfighting Architecture. [CG98]

NCW TECHNICAL CHALLENGES

The technical subsystems needed to realize network-centric warfare involve a significantly complex and varying set of requirements including security, mobility, quality-of-service, interoperability, robustness, bandwidth efficiency, and cost. These design requirements also often have broad ranging impact across vertical and horizontal architectural components. The underlying need for tradeoff consideration in such a complex interconnected environment is painfully familiar to experienced networking scientists and engineers working in the field. The well-known axiom *"good, fast, cheap; pick two; you can't have three"* illustrates the need to come to grips with competing design parameters and system requirements.

In this section, we consider a few of the design challenges related to networking that must be overcome to achieve the NCW vision, specifically: misplaced expectations; large-scale network design; and the impact of interconnection as it relates to the heterogeneity of legacy networks. We postulate that each of these factors creates friction that must be overcome in order to create the networking infrastructure to support NCW.

Misplaced Expectations

In many cases, the ubiquity of today's commercial Internet and cellular networks has created similar expectations for envisioned military networks. This has created the illusion that the network infrastructure supporting NCW is achievable by cobbling together various existing components. Such an expectation and oversimplified technical approach is problematic. A recent report by the National Research Council on the future of untethered communications [Goodman97], involving the input of leading

industry and military experts, concludes "a large gap remains between public expectations for *mobile* communications and the available technology." While the report also concludes that commercial efforts over the next 10 years will close some of the technology gaps, military application needs and requirements will likely exceed and differ significantly from anticipated core commercial developments. This should perhaps come as little shock when one considers the unique applications and environments driven by NCW. Unique requirements such as situational awareness, security, increased mobility, and heterogeneous wireless operation all contribute to increased friction and heightened challenges facing military network technologists of the future.

Large Scale Interconnection and Perceived Value

One of the quandaries faced by the designers and planners of the network infrastructure to support NCW is quantifying the benefits of future interconnection in advance of actual deployment. The necessity of quantifying such benefits is reasonable and necessary given the current and foreseeable defense budget climate. However, the detailed quantification of large-scale network design benefits is not well understood in large-scale commercial networks, much less within highly heterogeneous (mobile, wireless) military networks. Lack of detailed quantitative understanding is the key point here. The constantly changing application classes, traffic models, and dynamic multi-hop wireless network environments create a level of uncertainty and ambiguity in any analysis and scientists often grapple with complex simulation environments to predict potential performance impacts and behavior. Therefore, it is often difficult to fully quantify the benefit of interconnecting networks beyond certain broad predictive behaviors, qualitative benefits, and operational improvements.

Increased system interconnection and sharing also has its cost. After all, capacity sharing is a zero-sum game and if local communication resources are shared less resources may be available for local needs. Given the conservative nature, and for some good reasons, of those charged with ownership of the many heterogeneous military networks, why should significant local resources be spent on interconnection when such interconnection has the potential to reduce the network performance for the very mission for which it was designed? Therefore, network interconnection is often undervalued and network design is scoped to a degree where only direct localized benefit is obtained. Unfortunately, this limited scoping means that the full potential benefit of NCW is not obtained. To achieve NCW we must overcome frictional elements and scope designs more broadly, while still managing and supporting the needs of localized mission requirements.

Beyond Legacy Network and Application Designs

During an era of legacy computer and communication system development, system boundaries were well scoped and system design was often locally optimized for more limited mission requirements. We contend that continuing future system designs in this manner creates friction in an era of network centricity. Often solutions providing a highly localized design optimization may in fact be detrimental to the broader architectural needs. As an example, consider a quality-of-service (QoS) network design requirements (e.g., some bounded delay or guaranteed bandwidth reservation). A local system may support complex QoS signaling and management protocols and techniques to achieve the goal. The nature and behavior of these protocols may make the effective use of such a system in larger mobile system context or transactional application arena prohibitive and thus fall short of broader mission requirements. In this example, we have an indirect requirement conflict or competing sources of design friction.

In many cases, the original design of the network never anticipated the need for interconnection upon which NCW is based. Rather than view this deficiency in design for interconnection as a lack of fore thought on the part of the original network designers, this should be viewed simply as a response to the requirements as stated. The current state of heterogeneous military networks, and their lack of interconnection, is only in response to the user communities that benefit by their existence. Since the user communities, their applications, and their communications needs and platforms vary widely it is not surprising that the number of non-interconnected systems has proliferated.

Legacy networks were often designed for a limited number of nodes and types of traffic flows. While the initial designs are being pushed to larger number of nodes and types of traffic, the design flexibility necessary to interconnect effectively with unlike networks is rarely present. In addition to the cost and complexity of developing unique interfaces, the adaptation of legacy stovepipe systems can also necessitate the opening of interfaces that are proprietary to a particular contractor.

An additional source of friction is related to the original philosophy and experience of the network designers involved in developing military networks. We often see two cases. First, is the case where we begin with a specific radio system and attempt to evolve that into an effective distributed, information network. Second, is the case where we begin with a conventional, wired computer network and the associated protocols and applications and attempt to evolve these systems to operate in the mobile environment across a distributed wireless network. The starting points and legacy philosophies of the designers result in much of the difficulty in interconnecting such heterogeneous networks and making them ultimately interoperate efficiently and effectively. It is rare to find engineering experts that have a detailed understanding of both computer networking and wireless networking disciplines. Unfortunately, this is exactly the balance of engineering expertise required to address many NCW architecture issues and tradeoff challenges.

We provide another illustrative example of such potential friction by relating a story about a fictitious network application design. Imagine, if you will, a collaborative military network application originally conceived and developed by expert computer scientists. As a communication service, the expert computer developer chooses to adapt a well-known heavyweight, distributed computing protocol (codename *MagicBullet*) because this is what that particular computer networking industry understands and it works reasonably well in conventional bandwidth-rich networks. In our story, this same application is now being tested for deployment and must operate partially across bandwidth-limited and dynamic wireless networks within the battlespace to meet the mission requirements. It turns out that the end-to-end collaborative effectiveness does not appear to work well and the developer's cast blame at the wireless network for not providing robust, high bandwidth services. In actuality, are the heavyweight

distributed computing protocols to blame for the operational failure? Or, perhaps, does fault partly lie in the fact that the *MagicBullet*-based application and chosen networking protocols are now operating in an environment they were not originally intended or designed for with unforeseen consequences. Or, is it possibly the wireless system is truly a poor design that is not reasonably effective for supporting distributed, packet network communications and blame is justified. The likely answer is that all layers are contributing to the operational problem and therefore all layers should be considered contributors to the solution.

Our main point we hoped to illustrate with these examples is that often sources of design friction and potential broad deployment impacts may not be seen clearly from a localized or overly scoped design perspective. It should be noted that during network subsystem procurement and application development there is rarely a direct incentive to tradeoff network-wide system improvements --representing the larger operational community-- at the cost of some localized suboptimality or marginal increased complexity.

NETWORK DESIGN GUIDELINES

Here we examine further which technology building blocks have arrived, which are likely occur naturally in the coming years, and which areas likely need a research and development kickstart. As one example, the authors' believe that mobile and wireless networking technology -- the lifeblood of a dynamic battlespace information grid – likely needs further examining and focus to achieve the expectations set forth by the NCW vision. We now examine potential solutions and technology directions in several of these areas.

A Role for COTS Technology Integration

The NCW architecture will likely leverage future availability of small, low power, inexpensive network computing and wireless devices (in some cases, low cost throwaway items). In the future, such devices can be widely deployed to robustly and efficiently *self-organize* under dynamic conditions. The infrastructures formed by these *untethered* wireless computing devices can be adapted to serve a number of critical mission tasks, including platform-based communication networks, sensor networks, robotic applications, and low power wearable computing networks. In addition to being self-organizing and autonomous, this mobile computing machinery can be organized to provide the focused information handling processes required to support a desired mission. The devices envisioned could be integrated into other equipment or be completely self-contained and a set of such devices would serve to collect, process, distribute and disseminate information in an effective manner. It is also important that management of these *self-forming* information infrastructures should not be a hindrance to the task at hand; they should be as autonomous as possible.

It seems reasonable to assume from recent historical trends that commercial hardware will continue to become cheaper and faster (e.g., familiar Moore's law). In conjunction with that trend, software systems will become more complex and sophisticated and will be able to process, store, manage and disseminate larger volumes of information. What is not so clear is that related systems and protocols of interest for Department of Defense (DoD) application will be capable of operating in a self-organizing, auto-configuring, and adaptive fashion with the required environmental robustness and information utility. For example, the increased dynamics and resource constraints of wireless networks intensify the need for system efficiency, while the mission critical nature of shared information demands robustness, redundancy, and survivability.

Open Network Design: Localism vs. Globalism

Interconnection of networks implicitly creates a need for standards. This was one of the original motivations for development of the Internet protocol suite. Detailed areas of interconnection also need further understanding, development, and standardization. For example, what QoS mechanisms should be provided to allow traffic to flow across multiple heterogeneous networks to meet mission needs? Considering the requirement for mobility and security complicates this process further.

Consider the example of a sensor network connected to a tactical wireless network, such as the current Tactical Internet (TI), which is in turn connected by a satellite communication (SATCOM) link to an IP-based network cloud (Global Grid, Navy/Marine Corps Internet, etc). In this example, we assume the design of the sensor network is optimized for low energy consumption using non-IP network protocols specifically designed for such an environment. It also operates without traditional security mechanisms in place because of the unattended nature of sensor network. The tactical wireless networks uses IP-like protocols and applications that have been tailored for operation over low data rate wireless links with traditional military COMSEC/TRANSEC mechanisms. The IP network cloud is based on standard IP protocols, fiber optic communications links, and more standard security mechanisms.

Next, consider how information from the sensor network could be moved with QoS constraints on packet loss and latency through the tactical wireless network over the SATCOM link to a user or process that is part of the broader connectivity within the IP cloud. The traffic flow issue must be handled by three different flavors of network protocols, three different types of links (wireless terrestrial, satellite, fiber optic) each with distinctly different characteristics, and varying security mechanisms. Each of the three networks has been optimized in the past for performance as a homogeneous network. How will the QoS of the traffic described above be handled? The challenges associated with mission critical traffic that must flow across heterogeneous networks are daunting, but must be addressed for network centric warfare to become a reality.

One possible solution is that current and future networks should be budgeted and designed robustly with sufficient flexibility to accommodate future interconnection and applications that currently cannot be fully anticipated. For example, the Internet was not initially designed and conceived with user applications such as web browsers in mind. Yet, the flexible and scalable foresight of the IP protocol suite design eased the evolutionary deployment of new applications and transport mechanisms over several decades of deployment. Thus, a flexible design philosophy eases long term operational growth and supports novel applications that inevitably result once users have a chance to gain experience and fashion new doctrine.

In a broad sense a similar set of design problems and solutions were addressed during the early days of the first heterogeneous interconnection of computing systems, resulting ultimately in the modern Internet. The Internet Protocol (IP) suite of technology historically developed under an open, heterogeneous system design philosophy that is guarded and served in more recent times

in the form of such entities as the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF) [Leiner97]. The continued evolutionary development of effective protocols for a broad range of network applications and services and the continued health of the broad shared infrastructure has been of primary concern of these coordination watchdogs. The success of the Internet is proof of the power behind a scalable, heterogeneous networking design philosophy and the belief that the continued healthy operation and growth of the whole is an important design parameter.

Area-Based Building Blocks: Intersystem and Intrasystem

One of the challenges we have pointed out is one of addressing large scalability and heterogeneity within NCW. Network designers often use the concept of hierarchy and protocol layering to separate functionality and address problems across broad scales both horizontally and vertically. As an example, a two level hierarchy is commonly used to describe IP routing in the Internet. *Exterior gateway protocols* are used for routing between autonomous systems in the Internet backbone, while *interior gateway protocols* are used for routing within an autonomous system. The demands and requirements of these two routing functions differ significantly; thus, the preferred protocols for interior and exterior routing are typically not the same and may be significantly different in different areas of the network. These multiple solutions can be deployed simultaneously in separate areas of the Internet, while the Internet, as a whole, remains interconnected. This philosophy allows much of the organization of the network to occur from the bottom-up, as in the spirit of the NCW vision, with little or no disruption across the network as a whole.

In addition to defining autonomous systems and routing domains purely based on administrative authority, architectural boundaries between portions of an internetwork with significantly differing networking environments should also be considered. The NCW architecture depiction in Figure 2 clearly demonstrates some functional boundaries for consideration. It should be noted that this hierarchical design philosophy might find iterative application within an autonomous system to create autonomous subsystems, while at the same time continuing to support broad interconnections and interoperability. For example, within a force coordination network, possible boundary conditions might be the transition areas between significant tactical mobility or dynamics and the more static infrastructure areas. Defining multiple logical domains allows for the use of different protocols and services within different regions of an interconnected large-scale system, thus achieving the needed tradeoff between global and local optimization and allowing greater freedom for bottom-up organization of the network.

Autoconfiguration and Mobile Adaptation: Networks that just plain work!

Presently, there is growing interest in auto-configuration for quasi-static networks. Recent commercial endeavors are focusing primarily on end system configuration, since the number of end hosts typically far exceeds the number of routers in the overall system and end hosts are more often added or removed within commercial and business environments. Recently developed and emerging network protocols such as the Dynamic Host Configuration Protocol (DHCP) and the Service Location Protocol (SLP) are easing the burden of end system configuration. However, self-organization of the network infrastructure itself and auto-configuration of network routers, protocols, and applications remains a largely unexplored research area. In support of the NCW vision, significant portions of the military networking infrastructure need to be rapidly mobilized and deployed and are also likely to be highly dynamic with changing mission requirements once operational—increasing the overall burden of system configuration and management. The deployment issues and dynamics of the military scenario are unparalleled in commercial wireless networking applications; thus, it is unlikely that the commercial sector alone will be quickly driven to provide adequate solutions to these presently unique military environmental problems. While near-term solutions could focus on auto-configuration and mobile adaptation of existing protocols, longer-term solutions should consider new architectures, systems, and information handling mechanisms that adapt and organize. Related research should not be limited to initial protocol configuration performance issues, but should investigate adaptive protocol operation as the infrastructure behavior changes over time. Much like the initial military-based Internet technology investment, if shown to work, these techniques will find significant, future commercial application as well (e.g., factories, intelligent highways, disaster relief, emergency services, sensor systems).

The actual mobile networking and self-adapting technologies needed for NCW will likely vary with the particular mission requirements and environment of the subsystems under consideration. Once again, localized needs should be better understood in terms of mission requirements and appropriate protocols should be targeted. This will likely mean different solutions in different parts of the NCW architecture. As an example, routing protocol effectiveness is greatly influenced by mobility, distribution, and traffic characteristics of the users and the infrastructure [Perkins01]. Figure 3 provides an architectural snapshot of possible mobility classes within a network: end systems, infrastructure nodes, and aggregate subsystems. A broader discussion of evolving technology and related issues in interconnecting heterogeneous mobile systems is given in [MPC00].

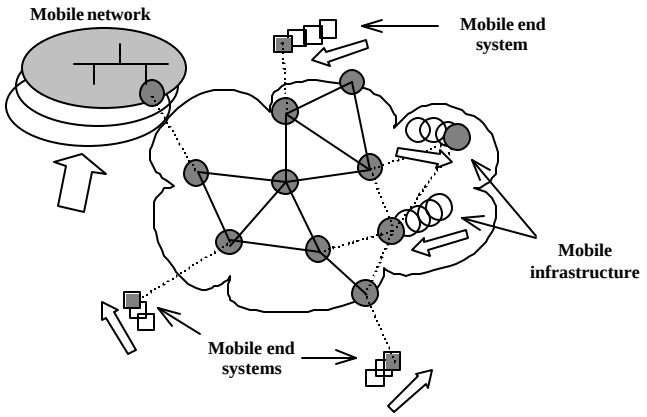

Figure 3: Varied examples of network mobility and dynamics

Heterogeneous Security Design

Preserving appropriate levels of network security is also a key component of the future NCW vision. Heterogeneous systems

within the NCW architecture have differing security requirements and policies and the interconnection and sharing of information between such systems is a complex design challenge. Once again we see a source of design friction, as security and other system requirements (e.g., mobile adaptation) present complex competing design requirements to the system architect. In our opinion, this problem should be attacked much the way network routing and mobility issues are attacked, by applying unique, appropriate solutions to satisfy local system and mission requirements and to use broader, open standard security building blocks to interconnect dissimilar systems where appropriate. Understanding and addressing the technical tradeoffs between security design, efficient networking techniques (e.g., multicast), mobility, and dynamic system adaptation will remain crucial to proper design of the NCW. As the network grows, security aspects begin to become more important to consider across multiple horizontal protocol layers and for varying application contexts (e.g., an appropriate application security mechanisms for e-mail may not be an appropriate solution for streaming media content and vice versa). Once again a new breed of security expertise is required that considers aspects of network architecture and mission application impact as a crucial part of the design.

Robotic and Sensor-based Opportunities

Emerging robotic and unattended vehicles and sensors present a new and unique opportunity to support a portion of the NCW vision [PM00]. Unattended ground sensor (UGS) networks may be the first of this new variety of networks to enter operational service. As envisioned, UGS networks are a unique type of network in that while having the ability to exchange information between other UGS nodes, the UGS node itself is not able to act in a meaningful operational sense based on the information a single (or even multiple) UGS node can obtain. Moreover, UGS networks serve a useful operational purpose only when the information obtained leaves the UGS network. Given that the UGS network will be battery operated, it is reasonable to expect that the UGS intra-network protocols will be optimized to minimize energy consumption. Despite, the necessarily unique design of the intra-UGS network protocol, the designer of an UGS network must take into account how the information obtained by the UGS can be exchanged with other non-UGS network nodes.

Broader Design Philosophy for Future Efforts

One of the difficulties in advancing the interconnection of heterogeneous networks with increased adaptation is that there is often no single owner of the greater network; there are only owners of the individual component networks. Also, the NCW vision warns against management centralization and promotes bottom-up organization. As an illustration, the Internet protocol balances this by giving the end system a significant role in the overall operation of the network, therefore creating some incentive for scalable and interoperable design. This present lack of broad ownership in military systems results in interconnection being given a low priority. Incentives need to be created to interconnect network in order to achieve the potential benefits of NCW. In many ways, advanced networking offers robustness and improved operational advantages to the user community, but these indirect effects may not be initial apparent. Also, the long term cost savings, flexibility, and maintainability of avoiding proprietary system interconnection and interfacing whenever possible should be an ongoing theme.

LOOKING BACK TO LOOK FORWARD

In promoting a way forward towards realizing NCW we believe that military technologists should look towards the lessons learned from the successful lessons of the past. The NCW vision "that significant improved operational power and mission execution can come through the increased timely sharing of information and system interconnection" is not a new theme in its technological concept. The several decades old Internet protocol suite development was orchestrated around the problem of interconnecting heterogeneous systems and allowing scalable information sharing amongst disparate systems [Kleinrock61, CK74]. In this case the dream has been realized and continues to evolve [Leiner97]. The difference in NCW lies not in the spirit of the vision and the needed design philosophies, but in the reality of the severe additional technical challenges of the unique applications, environments, and mission requirements of NCW. In that light, the value of a flexible, scalable design and innovation early on in the process should not be underestimated, nor should the need for significant awareness and consideration of competing architectural tradeoffs at many levels of the design.

REFERENCES

[CG98] A. Cebrowski and J. Gartska, "Network-Centric Warfare: Its Origins and Future," Naval Institute Proceedings, Jan 1998.

[CK74] V. G. Cerf and R. E. Kahn, "A protocol for packet network interconnection", *IEEE Trans. Comm. Tech.*, vol. COM-22, V 5, pp. 627-641, May 1974.

[Goodman97] D. J. Goodman, editor, "The Evolution of Untethered Communications," National Academy Press, 1997.

[Kleinrock61] L. Kleinrock, "Information Flow in Large Communication Nets", RLE Quarterly Progress Report, July 1961.

[Leiner97] B. Leiner, et al, *A Brief History of the Internet*, Communications of the ACM, Feb 1997.

[MPC00] J. Macker, V. Park, and M.S. Corson, *Mobile and Wireless Internet Services: Putting the Pieces Together*, IEEE Communications Magazine, June 2001.

[Perkins01] Charles Perkins, editor, *Ad Hoc Networking*, Addison-Wesley. 2001.

[PM00] V. Park, and J. Macker, "Protocol Considerations for Distributed Sensor Networks," NRL Memorandum Report, NRL/MR/5523—00-8521, Dec 18, 2000.