CHAPTER 11
Military Cyberpower
Martin C. Libicki

DOES CYBERPOWER, particularly military cyberpower, matter? This may seem to be an odd question: after all, do we ask whether airpower matters? But perhaps the question is not so odd. Airpower, when first introduced into warfare, was purely instrumental in its effects. In order to matter at that time, airpower had to (and still must) influence ground power. If airpower had zero effect on the ground—if it gave no capability to deliver supplies, drop bombs, or see something of value—then it would make scant difference that one's planes could fly anywhere at will and one's opponents' planes could not. The same is true for cyberpower. If control, influence, or competence in the medium has little to do with the delivery of military power in the more conventional realms,[1] then no one would need it, except perhaps for bragging rights.

To answer the question of whether military cyberpower matters, we first define *cyberspace* and hence, power in cyberspace, or *cyberpower*. Then we examine two experiments, one involving a Stryker Brigade Combat Team (SBCT) exercise, the other involving air-to-air and air-to-ground training sorties. We conclude that the available evidence so far does not allow us to reject the null hypothesis: that network-centric capabilities have no effect on mission effectiveness.

Distinguishing Characteristics of Military Cyberpower

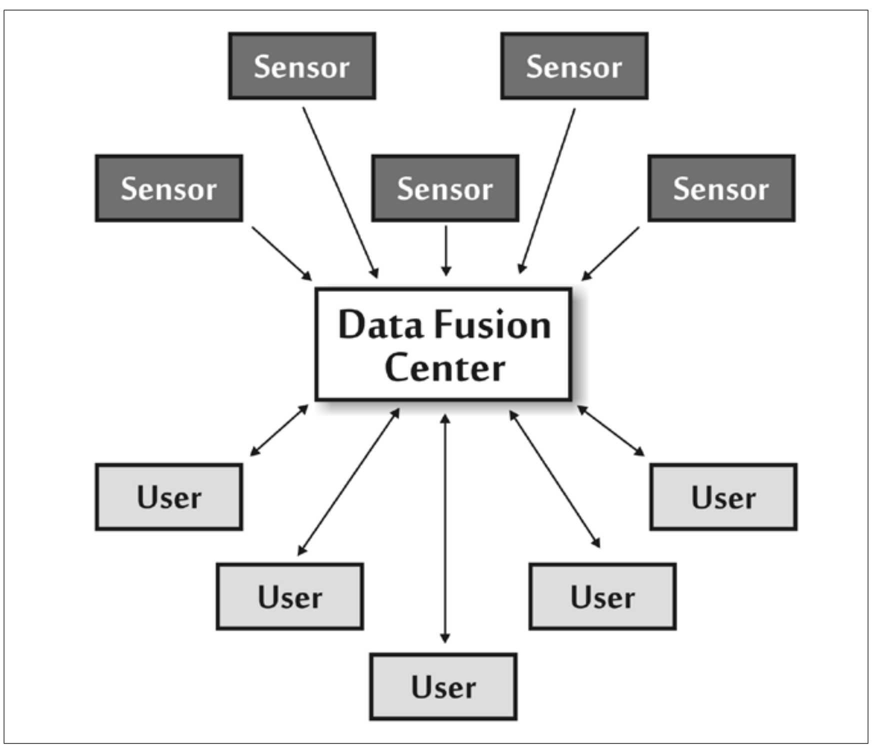
On the face of it, cyberspace would appear to be the pinnacle of domains. Cyberspace is all about information; while information has always been useful in warfare, it is now essential. However, cyberspace and information are not identical because the flow of information does not define a space. No one talks about "courier-space," "mail-space," "semaphore-space," or "telegraph-space," and certainly not in a wartime context. A definition of cyberspace presumes that changes in the quantity and speed, and more specifically the density and the interactivity, of information exchange imply a change in the quality of military information and decisionmaking.

Perhaps the best defining marker is that cyberspace is about networking, the two-way transfer of information, in contrast to broadcasting, in which information is transferred only one way. Networking appears to be the essence of cyberspace for two reasons: first, because *cyber* refers to control, and control requires feedback; second, because *space* assumes a medium in which there is omnidirectional movement, in contrast to the one-directional flow that would characterize water pipes. In other words, if there were no interactivity, there would be no cyberspace.

This distinction is crucial and is often ignored. Many advocates of military transformation through networking ascribe almost magical powers to its interactivity aspect, asserting that it will permit more agile command and control, enable warfighters to cycle through their observe-orient-decide-act loops faster than the enemy can, or allow self-synchronization, eliminating the need for hierarchical command and control and facilitating the superior tactic of swarming, thereby shifting power to the edge.[2] All of this takes interaction: the peer-to-peer exchange of information, perceptions, and plans. None of these effects would be possible, however, if the only noticeable result of networking the forces were to allow them to receive more information faster.

These oft-vaunted benefits of networking will not emerge if just a pair of broadcasting flows is mistakenly called networking. One good example of two-way broadcasting is Blue Force Tracker, a system by which every "blue" unit automatically transmits its global positioning system–determined coordinates to a data fusion center. The center amalgamates these location points, superimposes them on a map, and retransmits the completed picture back to all units. History suggests that such a capacity would be extremely valuable.[3] Similarly, networked sensors could feed a data fusion center, either directly or through intermediate nodes, which could collectively illuminate the battlefield and send a picture to inform the warfighters. Nevertheless, it would be misleading to call this the emergence of a new cyberspace, largely because absent peer-to-peer information exchange, there is no interaction space as such and no basis for more sophisticated (which may often mean less) command and control. Such a capability by itself would not push power to the edge, at least not directly.[4] In other words, the hourglass topology shown in figure 11–1 does not reflect cyberpower very well. The omninode or all-point connectivity topology shown in figure 11–2 is required.

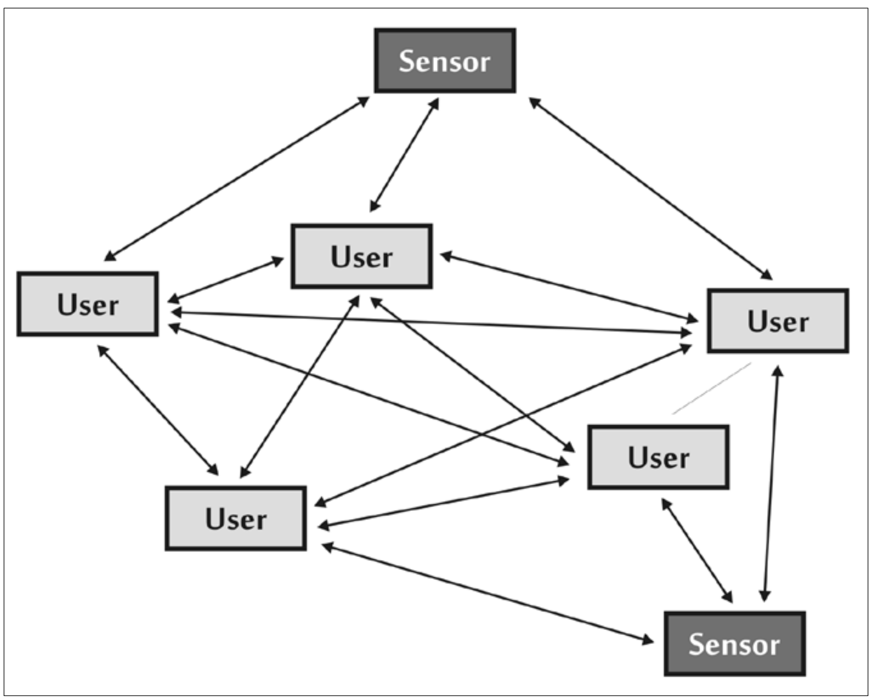
Figure 11-1 Hourglass Typology



We can now revisit the central question: does the creation of cyberpower by networking the operators permit a measurable improvement in operational effectiveness? To answer this question, we must rely on the results of experiments rather than actual combat results. Despite nearly two decades of discussion about the so-called revolution in military affairs (now called *transformation*), the digitization of the armed forces has been slow. Soldiers in the 2003 invasion of Iraq who operated below the company command level had very little digital connectivity; they were often first apprised of enemy forces the old-fashioned way, by running into them.[5]

As of May 2005, three networking experiments had been completed, and only two of them had produced anything quantitative that spoke to military effectiveness.[6] The SBCT experiment was documented in a RAND report.[7] The second experiment examined the effect of equipping Air Force pilots with networking capabilities (specifically, the Joint Tactical Information Distribution System [JTIDS], also called Link-16).[8]

Figure 11-2 All-point Connectivity Topology



Both experiments appear to show substantial performance improvements from networking. However, the important question is: What aspects of network-centric operations best explain the improvement? Is it the network as network, that is, cyberspace, or more simply that a network meant the ability to pass more information faster? If the latter—if it was access to information per se that made the difference—comparable improvement could be provided with something similar to broadcasting. If, however, cyberpower resulted in improved information-sharing and shared situational awareness—and hence better collaboration and thus some potential for self-synchronization—this would mean that cyberpower does, indeed, matter for military power. What we found, however, was that neither experiment convincingly demonstrated without ambiguity that networking made a difference in combat effectiveness.

Results from a Stryker Brigade Combat Team Experiment

The SBCT experiment was conducted during the Joint Certification Exercise at the Joint Readiness Training Center at Fort Polk, Louisiana, in early 2004. It contrasted the performance of two similar—but by no means otherwise identical—brigades. The SBCT had dense networking between and among all vehicles, while the light infantry brigade (LIB) did not. Each attempted to take an urban target that was defended by an opposition force with armaments similar to that of current U.S. brigades.

The differences in performance were quite dramatic. The LIB—a standard force in today's Army—was able to locate and identify fewer than 10 percent of the forces it fought prior to engaging them. The SBCT was able to locate and identify 80 percent. Decisions that took the LIB 2 days to make and transmit took the SBCT only 3 hours. The LIB took as many casualties as it imposed, but the SBCT enjoyed a combat exchange ratio of better than 10:1. In the end, the LIB did not take the town; the SBCT, by contrast, succeeded.

However, it is not clear that networking accounted for all or even most of these differences. Napoleon remarked that victory favors the larger battalions, and on that count, table 11–1 is revealing. Even without information technology, the SBCT's greater size would have given it a distinct combat advantage; it was particularly well equipped with snipers.

Table 11-1 Stryker Brigade Combat Team: Conventional Advantages

	Light Infantry Brigade (LIB)	Stryker Brigade Combat Team (SBCT)	Ratio LIB : SBCT
End Strength	2,705	3,498	1:1.3
Riflemen	1,062	1,353	1:1.3
Mortar Men	132	168	1:1.3
Snipers	18	51	1:2.8

The advantages of the SBCT do not end there. The Stryker vehicle itself had a level of firepower that the LIB lacked. Members of the LIB had to walk to the battle, 25 kilometers away, on a route with considerable potential for ambushes; the SBCT warriors had vehicles and could drive there. The SBCT thus arrived far more rested and ready for combat. Perhaps the most significant difference in terms of finding the enemy was that the SBCT had four times the number of reconnaissance units that the LIB had, and because they got there sooner, they had 60 hours available to do reconnaissance, while the LIB had just 42 hours. As a result, the SBCT had a 6:1 advantage in intelligence collection team–hours, so perhaps the 8:1 advantage in what they could find is not so surprising. Both sides had comparable use of advanced sensors: the SBCT alone had access to unmanned aircraft systems, but they were only used for confirmation of information gathered by other means.

The SBCT also enjoyed a vast advantage in connectivity. The LIB had FM radio and poor quality field voice equipment, while SBCT gear included the enhanced position location reporting system, near-term digital ratio, and satellite radios that could access military satellites and combat net radio operating over commercial channels. The SBCT enjoyed connectivity of 14 kilobits per second to every vehicle and 1.5 megabits per second to the brigade headquarters. The only equivalence between the SBCT and the LIB was in digital data connectivity to the dismounted soldier: zero in both cases.

Differences in numbers, firepower, and reconnaissance assets, as well as communications capability, meant that the SBCT had the option of pursuing different approaches to its objective. SBCT warfighters could use their superior reconnaissance and communications assets to avoid the two-thirds of the opposition force that was fielded outside of the town and attack the town directly. It was the SBCT and not the LIB that was able to find the best avenue of approach to surprise town defenders.[9] The SBCT was able to attack the town 13 hours earlier than the LIB could, destroy the enemy force as a fighting unit, and clear every building. By contrast, the adversary was able to mass its combat power against the LIB and thereby defeat the brigade in detail, resulting in overall mission failure for the LIB.

A closer look at some of the intermediate variables shows that the SBCT had superior knowledge compared to the LIB. Both teams were asked, after the exercise, whether the information each had was complete and accurate (most of the priority intelligence requests were "where" questions). Whereas the SBCT answered *yes* in 80–90 percent of the cases, the LIB could answer *yes* in only 10–20 percent. It took an average of 12 hours to get information to the LIB from spotters, but just 2 minutes to get similar information to the SBCT. The LIB had to allow 48 hours between the creation of a war plan and its execution to get the word out to its forces. The SBCT was able to do this in 3 hours and thus could attack the town early, achieving surprise.

Specific testimony taken from surveys of the participants underscored that advantage. One infantry battalion commander in the SBCT commented, "I could see on the Common Operational Picture that the lead battalion accomplished its mission early. I moved up our attack time to achieve momentum," and presumably he gained it. Many references to distributed planning, which was likely aided by networking, were made in interviews, but the testimony does not reveal whether the primary advantage of distributed planning was that planners had superior access to each other or they simply had faster access to more reliable data. For example, one participant said that "instead of focusing discussion on the base level of knowledge and comprehension of the situation, these interactions in the SBCT were observed to reach the higher levels of analysis and application." Similarly, a Joint Readiness Training Command observer noted, "The Stryker brigade [best] exemplified [this capability] with collaborative planning between the main [command post] and the tactical [command post]. . . . VTC [video teleconferencing] capability should be extended to lower echelons . . . to enhance situational awareness [and] understanding."

To assess this experiment, we start by attempting to rule out all the hypotheses that any or all of the non-network advantages were sufficient to cause the difference in outcomes.

The SBCT had clearly superior conventional forces: more (and better rested) soldiers and greater firepower. Historically, such a modest advantage is not unknown to result in an unambiguous win. Such a win, in the absence of overwhelming force differences, however, generally requires that soldiers on the losing side recognize what fate holds in store for them and bolt from the battlefield, suffering disproportionate casualties in the process. However, in neither case did either of the combatants lose cohesion (and why would they in an experiment?), so the advantage of superior forces has to be ruled out. When forces fared badly, they fared badly in detail. Thus, one has to eliminate superior conventional force as sufficient in itself to explain such vast disparities in outcomes between the SBCT and the LIB.

Another advantage was that the SBCT had time and resources to do six times as much reconnaissance as the LIB. The fact that it was able to find more of the enemy more quickly can reasonably be correlated with this advantage. However, it may be a bit of a stretch to argue that firepower and reconnaissance alone could explain all of the difference in outcomes. Perhaps it was the SBCT's ability to fuse data more efficiently into an accurate picture of the battlefield that was more telling. For example, the SBCT was able to acquire information from spotters far faster than the LIB could. Is a combination of firepower, reconnaissance, and data fusion—which is to say, firepower and knowledge to the warfighter—enough to explain the difference in outcomes? To know the answer, one would have to compare two identical SBCT teams, one that had only the hourglass networking topology of figure 11–1, and one that was capable of taking advantage of the all-point connectivity of figure 11–2.[10] That was not done in this experiment.

Consider, finally, the SBCT's advantages of faster command and of distributed planning. The problem from the analytical point of view is that, because we cannot rule out the possibility that the other advantages already discussed— firepower plus knowledge—could account for the difference in outcomes, we cannot rule out the possibility that network-centricity per se had no additional impact on the outcomes.

Results from the Air-to-Air and Air-to-Ground Case Studies

The experiment of equipping Air Force pilots with networking capabilities, specifically JTIDS, says even less about whether cyberpower enhances military power. This has less to do with the construction of the experiment, as in the SBCT case, and more to do with the nature of air operations. First, aircraft, being expensive platforms, have always been equipped with the kind of advanced communications that mobile ground forces could only dream of. Second, there are far fewer opportunities for the kind of network-mediated collaboration in the air than there are on the ground, for reasons that are easy to imagine: flying aircraft is a demanding activity that requires continuous attention to the machine. Furthermore, while multiple aircraft do work together, it has usually been in relatively small numbers, and the pilots are often within sight of one another. The advent of long-distance networking has removed the requirement of visibility, but the numbers of coordinating units are still relatively small.

The analysis compared the mission effectiveness of "voice only" F–15 flights to that of F–15s with both voice and JTIDS capability. Adversary aircraft were assumed to have the same attributes in both cases. This study, unlike the SBCT case above, had the advantage of a large data set: 12,000 training sorties. The data was gathered through a combination of quantitative metrics and calculations as well as pilot interviews, using conservative assumptions, to examine mission effectiveness expressed in terms of kill ratios.

The improvement in kill ratios with JTIDS was, if not the 10:1 ratio of the SBCT experiment, still an impressive result of roughly 2.6 to 1 (see table 11–2).

Again, we ask what aspect of JTIDS led to such improvement. Pilots cited eight factors in particular. Two factors arise from superior knowledge: earlier, more complete individual and shared situational awareness and understanding of the adversary air picture (information completeness included knowledge of one's own aircraft formations and of enemy aircraft); and information superiority in the sense of becoming more quickly aware of and more deeply understanding of enemy air formations.

Another cited factor results from being able to acquire such knowledge faster: more decision time available for flight leads (and wingmen) and thus a greater ability to focus on the fight itself and maneuvers antecedent to it. A fourth factor results from being able to acquire such knowledge earlier (that is, prior to engagement): improved battle management and targeting before engaging. A fifth factor resembles the classic network-centric formulation: better ability to self-synchronize, or "swarm."

The remaining three factors mentioned by the pilots are the practical (and inferred) consequences of the first five: better intercept geometries, improved lethality of missile shots, and more shots per engagement.

Tagble 11-2 Improved Kill Rates with Joint Tactical Information Distribution System

	Voice Only	Joint Tactical Information Distribution System (JTIDS)	Voice Only : JTIDS Kill Ratio
Daytime	3.10	8.11	1:2.62
Night Time	3.62	9.40	1:2.60

Both of these experiments indicate that one of the great values of networking is that it makes meetings more efficient: far less time is spent arraying and debating facts. This leaves far more time to generate and evaluate plans that depend on the observed facts. Whether better meetings lead to better warfighting, however, is another question.

One cannot, from this evidence, determine whether the one attribute that depends on the definitive characteristics of cyberpower—the ability to self-synchronize and swarm—has, by itself, a positive, null, or negative effect on the exchange ratio. It is reasonable to believe that the ability to "see" the target more quickly and earlier in the engagement cycle has an appreciable effect on mission effectiveness. It is certainly plausible, however, that the extra knowledge that is brought to the pilot through higher bandwidth and data fusion may itself account entirely for the effect.

A similar analysis applies to current and emerging capabilities for air-to-ground engagements. With JTIDS, the pilot has access to a map with potential targets indicated on it with *X*s. The presented information is not good enough for precision bombing (using joint direct attack munitions), but it suffices for weapons that have the capacity to acquire the target precisely on their own if told generally where to look. It may also be good enough to cue other sensors that might identify impact points more precisely. At any rate, if accurate, it is a good synoptic picture of the battlefield. In contrast, however, JTIDS can provide much clearer communications between the forward air controller and the pilot. Compared to voice commands, digital commands can provide more information that is more clearly indicated and more persistent in the aircraft's memory.

Here, too, networking leads to better information. Pilots get more detailed data from forward air controllers faster and more reliably. They also get a much more complete and up-to-the-minute picture of adversary aircraft. Whether this fits the definition of cyberspace, such that we can say cyberspace improves performance, is much harder to determine from these results.

Conclusion

Overall, the same conclusion (or rather, absence of a conclusion) arises from both the ground and air experiments. The evidence presented does not allow us to reject the null hypothesis: that network-centric capabilities have no effect on mission effectiveness once the ability of networks to efficiently transmit data, especially consolidated data, is taken into account.

Thus, the debate must continue over whether cyberpower—as manifested in network-centricity—has any positive effect on warfighting effectiveness. This is not entirely unprecedented for new means of warfare. Take airpower, for example. Few better examples of airpower can be given than the American and British use of it against Germany in World War II. Yet even now, considerable controversy remains over whether the expenditure of resources and blood— 50,000 dead in the 8th Air Force alone—could have led the war to a speedier end had it been devoted instead to ground forces.[11]

So it is with cyberpower. In years to come, the U.S. defense establishment may conduct further experiments that test the claims of net-centricity more carefully by allowing both sides to have identical access to knowledge, but allowing only one side to enjoy the technologies that promote collaboration or faster command in general. Until then, the null hypothesis—that cyberpower does not matter—remains to be disproved.

---

[1] The use of cyberspace to influence perceptions by carrying messages does not depend on other military media for its effect, but this is a different dimension of power and is not the subject of this chapter. For discussion of that dimension, see chapter 14 in this volume, "Cyber Influence and International Security."

[2] The observe-orient-decide-act loop is also known as the Boyd cycle, after Air Force Colonel John Boyd who first articulated it. See John Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston: Back Bay Books, 2004). On swarming, see Sean Edwards, *Swarming on the Battlefield: Past, Present, and Future* (Santa Monica, CA: RAND, 2000).

[3] Martin van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), dwells on the difficulty that commanders have had in simply knowing where their forces were.

[4] It might help indirectly, insofar as units that knew precisely where their cohorts were could coordinate actions better on a peer-to-peer basis, even if their means of communications were no more advanced than those available to U.S. soldiers in World War II.

[5] See David Talbot, "How Technology Failed in Iraq," *Technology Review*, November 2004.

[6] John J. Garstka presented a list of experiments in "Network Centric Operations: An Overview of Tenets and Key Concepts," presentation to the NCO Short Course at the National Defense University, May 18, 2005.

[7] David Gonzales et al., "Network-Centric Operations Case Study: The Stryker Brigade Combat Team," MG 267–1–OSD (Santa Monica, CA: RAND, 2005).

[8] Results drawn from briefing slides presented by Jack Forsyth, "Network-Centric Operations: Air-Air and Air-Ground Case Studies," delivered to NCO Short Course at the National Defense University, May 18, 2005.

[9] The report suggests that the Stryker Brigade Combat Team was able to deceive and thus surprise the town's defenders as well, but it did not explain whether their communications capabilities played a role in their being able to do so when the Light Infantry Brigade could not.

[10] To achieve statistical significance, one would have to run the experiment repeatedly with similar outcomes, as well as eliminating the Hawthorne effect (the tendency for people to perform better when they are subjects of an experiment).

[11] Richard Overy, *Why the Allies Won* (New York: Norton, 1996), makes the case that it was worthwhile because it forced Germany to waste resources on air defense that it could ill afford.