CYBERSPACE – THE FIFTH OPERATIONAL DOMAIN

Gen. Larry D. Welch USAF (Ret.)

The Problem

The concept of cyberspace as a domain has been in vogue for only a few years Still, extensive operations in cyberspace have been a reality for decades. Hence, while cyber operations are not new, our understanding of cyberspace as a domain requires further maturing.

Cyberspace as a Domain – Similarities and Differences

A more evolved, productive understanding of cyberspace can build on extensive experience in cyber operations and on similarities with approaches to operations in other domains. Though there are important dependencies in cyber operations impacting political, economic, and diplomatic activity, this article will concentrate on military activity in, through, and from cyberspace. For the rest of this article, the term cyber operations will include creating military effects in, through, and from cyberspace.

This article also emphasizes the similarities between dealing with challenges and opportunities in cyberspace and in the other operating domains – land, sea, air, and space. This is not intended to minimize the challenges in cyberspace but instead to emphasize the need to build on proven capability-development expertise – and on processes that have enabled a wide range of military force capabilities over the years.

The fundamental imperative for maturing understanding is to treat cyber as a place, not a mission. That is, cyberspace is a domain in, from, and through which military operations create intended effects. The fundamental military objectives relative to this domain are essentially the same as in the other domains, again – land, sea, air, and space. The primary objective is freedom of action in, through, and from cyberspace as needed to support mission objectives. The corollary is to deny freedom of action to adversaries at times and places of our choosing. The ability to do both provides for cyber military superiority.

There are other important similarities in the demand for and nature of military superiority in the five domains. Military operations do not depend on access and operations in all areas of the domain at all times. For example, maritime superiority requires control of selected areas of the seas at

It is no more possible to control all of cyberspace or all of the networks of interest at all times than it is to control all of air space or all of the maritime space.

all times and other areas only at selected times. Similarly, air superiority requires control of selected areas at all times and other areas at selected times. The same is true of cyberspace. Even so, there remains significant confusion about the concept of cyber superiority.

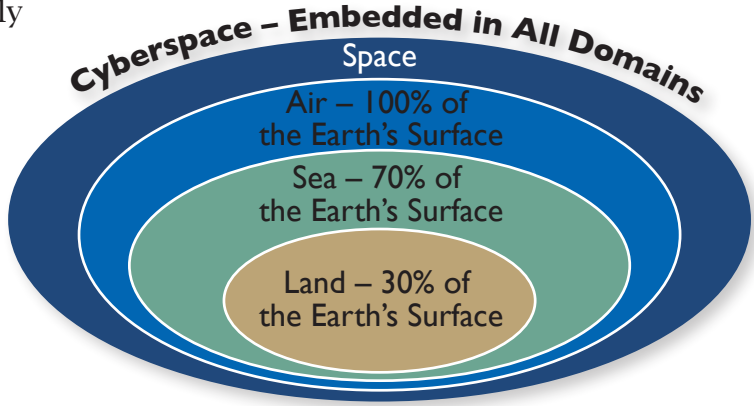

Figure 1. Cyberspace – the Embedded Domain

While there are key similarities, there are also fundamental differences between cyberspace and the other domains. One is that the hierarchy of other domains is geophysical in nature.

The hierarchy begins with the land surface of the earth surrounded by the maritime domain. All the land and seas are surrounded by the air domain, and the air domain is surrounded by the space domain. In contrast to the other domains as illustrated in Figure 1, cyberspace is embedded in all domains and operation in all domains is dependent on operation in cyberspace. Hence, military operations in all domains depend on operations in, through, and from cyberspace.

A second fundamental difference is that cyberspace is constructed by man and constantly under construction. It changes from moment to moment. Military interest in cyberspace is dominated by the use of networks for friendly and adversary operations. Most of the networks of interest are connected, leading to the perception that the cyberspace of interest to military operations is a single network. This is not a useful concept for cyber operations. It is no more possible to control all of cyberspace or all of the networks of interest at all times than it is to control all of air space or all of the maritime space. As is the case for other domains, the imperative for freedom of action in, through, and from cyberspace is to define the segments of cyberspace where such action is needed.

Missions in Cyberspace

The specific level and scope of the need for control of cyberspace is dependent on the specific activity conducted in, through, and from cyberspace. In general there are six classes of activities. They are:

- constructing cyberspace,
- passive defense,
- active defense,
- exploitation or operational preparation of the environment,
- attack, and
- defining the needed capabilities to conduct defined missions in, through, and from cyberspace.

Only the first activity is unique to the cyber domain. Unfortunately, the motivations driving construction of most of cyberspace did not include considerations of defense against cyber intrusion or cyber attack. Further, in addition to damage to forces and operations in the domain, cyber attacks can destroy mission-essential segments of cyberspace. Hence, defense in cyberspace includes freedom of action to conduct cyber operations impacting operations across the domains, protecting access to the needed segments of cyberspace, and protecting the existence of those segments of cyberspace. The adversary cannot destroy segments of the air, sea, or space. The adversary *can* destroy segments of cyberspace.

Cyberspace may also be unique in the breadth of effects from cyber operations. Dr. Richard Ivanetich recently suggested to me that it is useful to think of the range of effects as physical, logical, or cognitive. In the physical realm, the effects can include causing physical damage by causing physical assets such as power generation to self-destruct. In the logical realm, the effect can be disrupting functions essential to computer control of the networks, information flowing or stored in the networks, and/or the decision support systems supported by the networks. The cognitive effects include the strategic influence aspect of information warfare impacting the decision processes and capabilities. This range of effects can be generated with attacks against adversaries. They can also be part of the challenge of defending against adversary cyber attacks.

Priorities for Meeting Challenges and Leveraging Opportunities

The similarities and differences suggest a set of priorities for meeting the challenges and leveraging the opportunities in cyberspace to meet mission demands.

The first priority is to identify those segments of cyberspace where freedom of action is essential to mission accomplishment. This does not start with an attempt to map the network. It starts with identifying the decisions required to conduct and support operations. This is followed by mapping the information collection, manipulation, storage, and movement required to support the decisions. When these two needs are understood, those segments of cyberspace (networks) essential to operations can be defined. This process will require an attitude of constraint. Given the current cyber culture, the demand will remain unconstrained unless a new level of discipline is imposed. While every decision maker from the platoon leader to the joint task force commander can make a case that unfettered access to information wherever it resides in cyberspace is essential to the effectiveness of his or her operation – an unconstrained approach based on these demands would virtually guarantee that, in the face of adversary cyber operations, every decision maker will suffer from loss of effectiveness due to the vulnerabilities of mission-essential segments of cyberspace.

The next priority is to focus on making those networks sufficiently defensible to ensure continued,

even if degraded, support for operations in the face of attacks on access, information, or the network itself. There is a perception that currently constructed cyberspace is so vulnerable that there must be a hedge to operate without access to cyberspace. The time when such a hedge was feasible passed at least a decade ago. It is no more feasible to conduct military operations without access to cyberspace than it would be to operate without access to the seas or the air. Instead, the focus needs to be on ensuring that selected segments of cyberspace are defensible, defended, and sufficiently robust to function under attack. This may require giving up some of the characteristics of the use of cyberspace that we have come to expect in our daily lives. It may require a drastically reduced number of gateways to essential networks. It may require active defenses that produce collateral damage to non-combatants whose resources are being used by adversaries to attack our operations and conduct their own. It will certainly require a combination of passive and active defense capabilities that respond at the speed of the networks and the clear and timely authority to use those capabilities.

The next priority is to develop and field the cyber forces needed to support the six classes of activities in cyber operations.

Building Cyber Forces

There is a perception that developing forces with cyber capabilities is a unique process understood only by cyber experts. The reality is that the process required to build forces with cyber capabilities does not differ greatly from the complex process of building the capabilities required to operate a Modular Brigade or an Aegis Cruiser or a Fighter Wing. In each case, the process is similar to that shown in Figure 2. It does take special understanding of each cyber activity to define missions, describe the desired

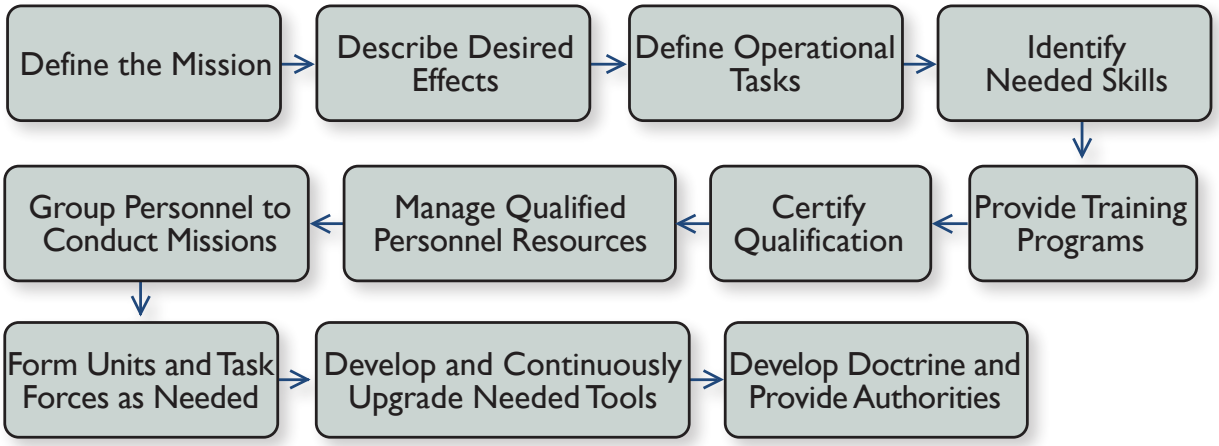

Figure 2. Force Building Process

effects, define operational tasks, and identify needed skills. Each class of activity requires a specific set of skills, tools, concepts, doctrines, and authorities. Still, the process is similar to complex processes that the military departments and defense agencies have successfully executed for a wide variety of new capabilities.

The point of Figure 2 is not to precisely describe either the sequence or the details of the force building process but to illustrate that it is a set of activities that the military departments and defense agencies know well and have performed successfully for decades. The military services have adapted to new demands, new environments, and new capabilities on a regular basis. Adapting to the demands of cyber operation is no more difficult than adapting to the change from the cold war to the post-cold war – adapting to the change from force-on-force operations to counter-insurgency and post-conflict operations. The issue now is to move forward rapidly to build the needed cyber forces with the needed set of capabilities to produce the desired set of military effects across the spectrum of cyber operations.

Operational Gain-Loss Concept

The cyber domain exacerbates a long-standing set of perceived and real conflicts in gain-loss decisions impacting operations. The conflict between the gains to an ongoing combat operation from denying an adversary the use of cyberspace at times and places of our choosing and the gain from exploiting the adversary's use of cyberspace is compounded by two factors. The first is a perception that combat operations and intelligence gain-loss are of interest to two different communities; therefore, there is conflict between communities – combat operations and intelligence. The second complicating factor is that adverse activities inside networks created by adversary action, insider threats, or inadequate attention to security measures can threaten the continued operation of a larger set of networks with consequences greater than the risk to an ongoing combat operation. Again, there is an inevitable conflict between the current combat operations gain from continued network operation and the loss risk to the network. Once again, this has been perceived as a conflict between two activities – current combat operations and network operations. The reality is that intelligence gain-loss, network gain-loss, and combat operations gain-

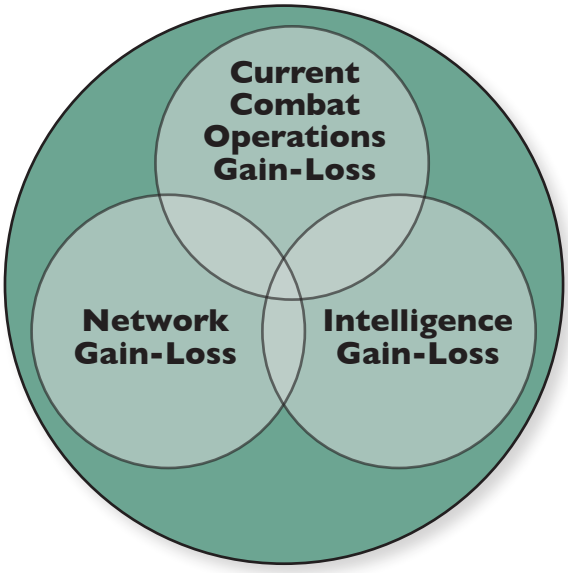

Figure 3. Operational Gain-Loss from Integrated Gain-Loss Considerations

loss are all operational matters and the operational commander responsible for the success of the joint operation needs to fully understand the full set of gain-loss risks and be the primary influence on gain-loss decisions. Operational gain-loss considerations must integrate a complex set of overlapping gain-loss considerations as illustrated in Figure 3.

At present, there is a structure and process to resolve intelligence gain-loss issues and an arbitrary practice to resolve network gain-loss issues. The current structure and processes do not integrate the gain-loss considerations as part of an overarching operational gain-loss decision process. This can have a wide range of serious consequences for military operations to include the loss of forces and failure in combat operations. Lack of a full understanding of such decisions can also have serious consequences for the intelligence information needed to support operations and for critically important networks and other critical infrastructure.

Further, many gain-loss decisions cannot await a complex set of processes. The need to deny adversary use of some segment of cyberspace may be the difference between success and failure of an ongoing operation and the cost of failure may be severe. At the same time, an adversary's exploitation of a network weakness could propagate to a wider network at Internet speed. Hence, there will need to be carefully defined rules of engagement, priorities, and authorities for timely gain-loss decisions.

Effective military operations have been increasingly dependent on cyber operations for several decades. The most fundamental objectives in cyberspace are similar to the objectives in the other domains – land, sea, air, and space. The objectives are freedom of action to create desired military effects and ability to deny such freedom of action to adversaries at times and places of our choosing.

Effects in, through, and from cyberspace include constructing defensible segments of cyberspace (networks), defending essential segments of cyberspace, exploitation, and attack. Attack capabilities can include creating physical effects, disrupting logical operations, and creating cognitive effects. Defense capabilities need to also deal with this range of effects.

While the needed skills, tools, and authorities are different for cyber operations, the processes needed to build effective capabilities are similar to those that the military departments and defense agencies have used to build other capabilities. The need is to do the complex, detailed work. There are no silver bullets.

The long-standing need to integrate intelligence and network gain-loss considerations into the overarching operational gain-loss decision process remains unfulfilled. The consequences can be loss of military forces, combat failure, loss of essential intelligence information, and/or high consequence damage to critically important networks.

General Welch is a former chief of staff of the U. S. Air Force and former president of IDA.