Building The Cyber Warfare Force

Larry Welch

The Challenge: Cyberspace may well be the most contested operational domain and the domain in and from which operations produce the most far-reaching effects in the land, sea, air, and space domains. DoD needs dedicated cyber operational forces provided by the Services and employed by combatant commands with clear warfighting missions.

Eight years after establishing USCYBERCOM, there remains a need for a clear mission identity across DoD, more clarity in military department responsibilities for force building, and more rapid growth in capabilities.

The Central Issue

Organizing for effective cyber operations serving the needs of the Department of Defense (DoD) has proved to be challenging. A particularly visible current issue is the future organization of United States Cyber Command (USCYBERCOM). The President has made the decision to elevate the command to a full combatant command, which will remove it from United States Strategic Command's (USSTRATCOM) jurisdiction, where it was to be integrated with other global missions. The second decision, now resting with the Secretary of Defense, is on separating the roles of Commander, USCYBERCOM and Director of the National Security Agency (NSA). This issue calls for a deeper understanding of the relationship between the cyber operations role of USCYBERCOM and the signals intelligence mission of NSA and of the impact of that relationship on both missions. Regarding organizing for cyber operations, there is a need for increased clarity in the answer to the fundamental question: "Organize to do what?"

To respond rapidly to the clear need for effective cyber operations, DoD initially elected to build cyber forces largely in or closely associated with the existing intelligence and information systems structure. That approach has produced significant new cyber operations capabilities. Still, 8 years after establishing USCYBERCOM, there remains a need for a clear mission identity across DoD, more clarity in military department responsibilities for force building, and more rapid growth in capabilities. The answer to the question "To do what?" is to structure forces, policies, and authorities to conduct cyber warfare securing vital elements of cyberspace and delivering combat effects in and through cyberspace. *The fundamental need is for a Cyber Warfare Force to conduct offensive and defensive operations.*

Some History

The initial motivation, advocated by the Director of NSA supported by the Director of National Intelligence, was the growing awareness of the need to protect information and systems from cyber intrusion and attack. DoD responded to the need by adding cyber operations to the mission responsibilities of USSTRATCOM. The Commander, USSTRATCOM's approach to this, and other missions added to the command's core strategic deterrence and space missions, was to form a set of Joint Functional Component Commands (JFCCs) and a Joint Task Force (JTF). This was to provide the command with access to needed expertise not available in the command.

The Intelligence Community's missions had long required intense focus on understanding information networks and exploiting access to information through networks. Forming JFCC-Network Warfare, with the Director of NSA dual-hatted as commander, was a logical organizing step in 2005. At the same time, Joint Task Force-Computer Network Defense (JTF-CND), created in 1998, was changed to Joint Task Force-Global Network Operations (JTF-GNO) charged with defense of the Global Information Grid (GIG). This separation of the offense and defense missions endured until the JTF-GNO was integrated into USCYBERCOM in 2010.

In 2008, the Deputy Secretary of Defense and the Vice Chairman, Joint Chiefs of Staff, asked IDA to provide recommendations on organizing for command and control (C2) of cyber operations. IDA formed a group of senior retired military officers and analysts who had relevant experience to address the issue. While providing options for approaches to cyber C2, IDA concluded and reported that DoD needed to put more emphasis on defining the cyber mission and building effective cyber forces than on C2 of forces not yet formed. Still the outbrief to the Joint Chiefs led to a decision by Secretary Gates to form a subunified command under USSTRATCOM, with the Director of NSA dual-hatted as commander.

The Commander, USSTRATCOM expressed the belief that the emphasis should be on clarifying mission expectations and on force building. He was concerned that building a new combatant command could be a distraction from needed clear direction to the military departments to deliver needed cyber forces. It soon became apparent that effective C2 has less to do with headquarters organization than with clarity of mission, authorities, force capabilities, and integration with operations in and from other domains. These essential elements are yet to be adequately defined and developed.

Expectations and Outcomes

Both the Commander USSTRATCOM and the IDA panel were concerned with the direction and pace of cyber capability development in DoD. By 2007, the Department was beginning to treat cyberspace as an operating domain, and in 2011, cyberspace was officially recognized as a contested operating domain. Given that recognition, military objectives are essentially the same as for the other four operating domains: access and freedom of action to deliver desired

effects in and from the domain at times and places of our choosing. The corollary to that purpose is to deny the same to our adversaries. The logical expectation was mounting a concerted campaign to define and build a Cyber Warfare Force to meet the challenges to national security. These challenges have long been widely experienced with the sure prospect of becoming ever more consequential. Defining needs is a key joint community role in force-building for any domain—answering the "to do what?" question. The military departments then have the role of organizing, training, and equipping forces to meet those needs.

In the case of cyber operations, this role applies to each of the military departments. Unlike other domains, given the ubiquitous nature of cyber operations and the impact on operations in and from all domains, there is no dominant Service in this domain. This need not be an obstacle to the set of force providers (military departments) building an effective Cyber Warfare Force. As an example, while there is a dominant Service in the air domain, each of the Services has organized, trained, and equipped air domain capabilities, tailored to their dominant domain, to meet the demands of joint combat operations.

To build capabilities rapidly, the Army placed the cyber force-building responsibility in the Army Intelligence and Security Command (INSCOM). The Navy put the responsibility for operational control to execute cyber, electronic warfare, information operations, and signals intelligence in Tenth Fleet. The Air Force started with an intelligence wing and information warfare center, which was moved from the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) to a newly formed 24th Air Force in Air Force Space Command.

The necessary initial reliance on the NSA cryptologic platform for essential cyber operations further tied military cyber operations to Intelligence Community limitations and priorities. Operations on this platform are essential to effective intelligence operations. Important processes and qualifications are required to ensure continued effectiveness for intelligence collection and support to the broad range of operations that includes cyber operations. The overall result was that force-building direction, including operating unit structure, training requirements, and certification, migrated to the newly established combatant command and was strongly shaped by Intelligence Community practices and priorities.

This force-building approach has produced significant cyber operations capability, but it continued for almost a decade with the inherent limitations of embedding a combat forces mission in a structure dominated by the intelligence and information systems communities. The joint and Services intelligence and information systems activities serve vital purposes and meet a challenging set of mission demands. They are not combat operating forces that must interface and integrate with combat operations across multi-domains. Such forces need the clear identity and career field opportunities and expectations that characterize the recognized combat forces of the Services.

The Army began to treat cyber operations as combat arms with the establishment of MOS 17C, Cyber Operations Specialist, in 2015 and now treats cyber operations as a distinct branch of the Army. For the Air Force, cyber superiority is still not treated as a core mission, and career management leadership for specialty codes making up the Air Force cyber mission force rests with the intelligence directorate and the Chief Information Officer. The Navy continues to embed cyber operations in the signals intelligence structure.

The Continuing Need

Effective cyber operations are increasingly essential to effectiveness in, from, and across all five domains. DoD is engaged every day in operations against aggressive adversaries in cyberspace. Cyber operations delivering effects in and from the contested cyber domain is a combat forces role. Meeting the operational challenge requires an operational organization with an operational orientation.

Intelligence and information systems skills and understanding are essential enablers of effective cyber operations. Intelligence officers and enlisted are essential members of combat operating teams—offense and defense. These skills are more essential for cyber operations than for other missions. Addressing cyber targets requires extensive intelligence preparation and continuous network analysis to navigate to the cyber target, penetrate defenses, create the desired effect, and assess the results. Further, unlike operations in other domains, cyber operations can change this man-made domain in hard-to-predict ways, requiring network analysis to be in real time.

These and other factors demand closely integrated, multi-discipline, experienced cyber combat crews in tailored units in the Cyber Warfare Force. The need is not to reduce the intelligence and information systems roles in cyber operations: the opposite is true.

The need is for a career force fed and sustained by communications, information, and intelligence career fields. But it cannot be a pick-up force of people temporarily diverted from other information systems and intelligence activity. Instead, it needs to be a Cyber Warfare Force treated as combat forces, managed and led as a career force. Like the approach to every other combat mission, the military departments need to deliver forces for cyber warfare operations conducted by combatant commands integrated with other forces to achieve warfighting effects.

The need is also for operating platforms and cyber weapons with capabilities and processes that are optimized for cyber operations. The operating platforms and cyber weapons need to provide for operations across the spectrum, from strategic to tactical. The rules of engagement and authorities need to be appropriate to the level of operations, just as is the case with operating platforms and weapons employed in and from other domains.

Conclusion

Cyberspace may well be the most contested operational domain. It may also be the domain in and from which operations produce the most far-reaching effects in the land, sea, air, and space domains. To deal with these conditions and consequences, DoD needs dedicated operational forces provided by the Services and employed by a combatant command or commands with clear warfighting missions.

The force capabilities need to include intelligence and information systems experience and expertise, but they cannot be effective if they are subordinate to intelligence or information systems authorities and priorities. DoD has been successfully defining needs and organizing, training, and equipping warfare forces for decades in the land, sea, and air domains.

The Department is addressing the reality of warfare in the contested cyberspace domain with increased intensity. Despite the continuous ongoing conflict in cyberspace and the near certainty that such conflict will have an ever-larger role in warfare at all levels, the term *cyber warfare* continues to generate resistance in some quarters. Still, the importance of the cyberspace domain to success in all domains clearly warrants intense attention to Cyber Warfare Force organization, capabilities, policies, and authorities.

General Larry Welch is a Senior Fellow and former President of IDA. He holds a Master of Science in international relations from George Washington University.