Guest Editorial

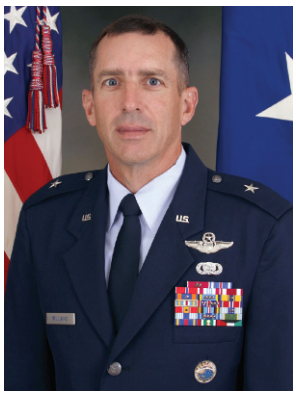
ITEA Journal 2010; 31: 439–441

The Imperative for Shaping Cyberspace

Brig Gen Brett T. Williams

HQ USPACOM, Director Communications System (J6), Camp H.M. Smith, Hawaii

The hot topic in the Department of Defense (DoD) today seems to be cyber, cyber, and more cyber. At the most senior levels, there is significant discussion and debate on the best way to Command and Control (C2) cyberspace operations. Given our reliance on cyber for executing C2 of military operations, this attention is well justified. Unfortunately, our efforts are not always well focused or synchronized, and despite the expenditure of significant resources, we do not yet have a comprehensive plan that addresses our biggest challenges in the cyber domain.



Brig Gen Brett T. Williams

The military imperative for gaining C2 of cyberspace operations comes from the Joint Force Commander's (JFC) requirement to execute C2 of C2. The term "C2 of C2" was coined by Admiral Robert Willard to describe the operational necessity of having Command and Control of the Command and Control architecture. The Admiral's argument is that C2 is what a commander does—it is his contribution to winning the fight. In order to execute his C2 mission, the commander must have a firm understanding of the technology he relies on to make decisions, direct operations, and manage risk. Although not all of the C2 architecture falls within the cyber domain, today's network-centric JFC relies heavily on cyberspace; therefore C2 of cyberspace operations is critical to his ability to execute C2 of C2.

Each Combatant Commander (COCOM) has a position on the best way to execute C2 of cyberspace operations within his area of responsibility (AOR). At the same time, the activation of U.S. Cyber Command (CYBERCOM) has created the impetus to clearly define our doctrine and policy for cyberspace across the DoD enterprise. Defining the proper supported–supporting relationships between the COCOMs and CYBERCOM, Defense Information Systems Agency (DISA), National Security Agency (NSA), and the Services is essential for determining how we are going to execute cyberspace operations in support of mission objectives. Unfortunately, we find that our C2 options are limited by the architecture that defines cyberspace. Cyberspace is a disparate collection of networks, systems, and software that nobody completely understands. It was never designed for military C2, yet we rely on cyberspace to execute the full spectrum of operations from humanitarian relief to warfighting. The Global Information Grid (GIG) as currently constructed severely limits our C2 choices, is too difficult to operate and defend, and costs more than it should. We built cyberspace. We can and should change it.

The professionals of the test and evaluation (T&E) community are well aware of the mad rush to gain complete awareness and control of cyberspace. There are numerous funded and proposed projects focused on cyberspace operations, yet we seem to be missing a roadmap to tell us where we are going. In other words, from a DoD perspective, what should cyberspace look like in the future if we are going to rely on it for national security?

GIG 2.0 is the most recent roadmap. It was introduced in 2008 with the intent of providing the warfighter with an "information advantage." GIG 2.0 focused on five areas: (a) global authentication, access control, and directory services; (b) information and services "from the edge"; (c) joint infrastructure; (d) common policies and standards; and (e) unity of command. GIG 2.0 provided useful motivation for improving our ability to operate in cyberspace, but it did not address the key challenge we face: "It's all one big GIG, so a risk assumed by one is a risk assumed by all." The lack of boundaries in cyberspace means that when the JFC directs operations in cyber, he must always consider the impact on the rest of the GIG. This is a different dynamic than exists in the physical domains, and it drives us to C2 relationships and operational decision making centralized at the DoD level. Additionally, the "one big GIG" factor makes computer network defense (CND) and network operations (NetOps) more difficult, leading some to

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Imperative for Shaping Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **HQ US Pacific Command (USPACOM),J6,Camp H.M. Smith,HI,96861**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**3**	

focus disproportionately on offensive cyber activities. It is time to update our roadmap and lay out a plan to purposefully shape cyberspace. It is time for GIG 3.0.

The proposed GIG 3.0 capitalizes on existing virtualization techniques to create a cyber Joint Operating Area (JOA) that allows the JFC to execute C2 of cyberspace operations in the same way he executes air, land, maritime, and space operations. GIG 3.0 is a deliberate and proactive game plan to shape cyberspace into a defendable, robust, agile, and secure environment that guarantees friendly freedom of action and denies the same to the enemy.

The basis for GIG 3.0 is a new network environment based on current Multi-Protocol Label Switching (MPLS) technology. This new network environment would be established within the current Defense Information System Network (DISN) and provide the network layer for cyber JOAs—a concept we have defined as the operational network domain. Operational network domains would be created using a set of controlled interfaces to define and separate, from the rest of the GIG, the cyberspace assets and infrastructure that directly support a given operational mission. The controlled interfaces would manage and contain risk in support of the JFC's intent without passing that risk on to the rest of the GIG. At the same time, CYBERCOM and the Services, via the same controlled interfaces, would administer their GIG-wide responsibilities within the JFC's operational cyber domain. An operational network domain would allow the JFC to direct operations and assume risk in his "cyber JOA" just as he does in his geographic JOA. Operational network domains would be flexible, adaptive, easy to establish, and could be controlled via a wide variety of doctrinal C2 constructs.

Within and across the operational network domains, virtual secure enclaves (VSE) would be created using existing commercial off-the-shelf technology (COTS) that has been certified for protecting classified information. These COTS systems use Internet Protocol Security (IPSec) encryption techniques that simplify information sharing with coalition partners and reduce the cost and complexity associated with controlling classified infrastructure. The enclaving strategy also allows us to define key terrain and avenues of approach in cyber, so we can precisely focus our sensors and intrusion analysis to significantly improve our capability for CND and NetOps. Like the operational network domains, VSEs would be extremely agile and would require minimal time to establish. In addition, we would be able to quickly shift services between VSEs to mitigate the effects of physical or logical failures and to enable advanced computer network operations. Finally, the VSEs would employ dynamic electronic keying techniques to facilitate rapid, secure changes to the community of authorized users.

The final component of GIG 3.0 is the Multi-Enclave Client (MEC). The MEC is a work station that allows the user to access multiple VSEs. Currently, most users who require access to several different networks require multiple workstations. The IPSec VSE environment provides the opportunity to employ already approved MEC solutions to access both classified and unclassified networks from a single computer. MEC workstations offer a streamlined method to access information. They reduce costs because there are fewer machines and less supporting infrastructure. And, they offer the potential to reduce overhead because there is less equipment to deploy, and the power requirements are reduced.

Creating enclaved cyber JOAs and accessing them using efficient multi-enclave workstations is only part of the GIG 3.0 roadmap. All of this technology is wasted if we do not develop appropriate tactics, techniques, and procedures (TTP) to take advantage of the technology and the T&E community has a key role in the process. Joint TTP are necessary for operations in every domain, especially cyber. Established TTP allow the commander to issue orders with confidence knowing that the forces assigned to him will execute their mission in a predictable fashion. As with the earlier discussion on C2 options for cyber, it is important that we do not allow the current architecture to restrict our TTP development for cyberspace. There is a synergistic relationship that must exist between technology development and the maturation of cyber TTP. The T&E community should help ensure that there is close integration between the technical experts and the operational community as we develop GIG 3.0. The fact is that the officials in DoD who have the most impact on cyber policy and resources do not typically have the background to advocate for specific technologies. At the same time, the technical experts, who do their best to meet operational requirements, do not always understand the relationship between the technology and the mission. Our test directors have a responsibility to help ensure that these two communities are closely coordinated and aligned as we develop the cyberspace of the future.

Doctrine, policy, C2 relationships, and TTP for cyberspace operations are just as important as they are for operations in the physical domains, but cyberspace is different. It is a domain that comprises live, virtual, and constructive assets that provide real capabilities. We do not completely understand the nondeterministic nature of the cyber domain, but we know we must, and, as a result, we are frantically searching for

ways to execute cyber operations just as we do operations in any other domain. We would like to get to the point where we do not need a separate construct for cyberspace, but for now our perception of the domain and the design of the architecture are forcing us to treat cyber as a special case. We have an urgent imperative to shape cyberspace in a way that we have never done before. The T&E community has a key role in guiding our many disparate efforts, so that in the end the cyber domain meets the requirements of the JFC. ❑

Brig Gen Brett T. Williams is the Director, Command, Control, Communications and Computer Systems, U.S. Pacific Command, Camp H.M. Smith, Hawaii. He is responsible for the communications system across the largest regional combatant command enabling joint and coalition operations. He provides senior leadership and management of Pacific and global communications resources to support the headquarters and the forces of four component commands, four sub-unified commands and all joint task forces.

General Williams was commissioned in 1981 as a distinguished graduate of the ROTC program at Duke University. He is a graduate of Euro-NATO Joint Jet Pilot training and the U.S. Air Force (USAF) Fighter Weapons Instructor Course. He has commanded a fighter squadron, combat operations group, and two combat wings. The general was the Air Combat Command Inspector General, a plans officer at U.S. Central Command, and Chief of Checkmate Division on the Air Staff at the Pentagon. Prior to his current assignment, he was the Commander, 18th Wing, Kadena Air Base, Japan.

General Williams is a command pilot with more than 3,600 hours in the F-15C and more than 100 combat missions in operations Desert Shield, Desert Storm, Southern Watch, Northern Watch, and Iraqi Freedom. He was promoted to Brigadier General in October 2007. He earned a bachelor of science degree in computer science from Duke University, Durham, North Carolina, in 1981 and a master of arts degree in management from Webster University in 1988. In addition, he completed the USAF Fighter Weapons Instructor Course, Nellis Air Force Base (AFB), Nevada, in 1989; and attended the Air Command and Staff College in 1993 and the School of Advanced Airpower Studies in 1994 at Maxwell AFB, Alabama. In 2002, General Williams completed the Advanced Strategic Arts Program at the U.S. Army War College, Carlisle Barracks, North Carolina.

General Williams is currently the Director, Command, Control, Communications and Computer Systems (J6), U.S. Pacific Command, Camp H.M. Smith, Hawaii. E-mail: brett.t.williams@pacom.mil