Cyber Vision and Cyber Force Development

Kamal Jabbour, ST

Widely reported compromises to the Department of Defense global information grid (GIG) punctuate a recent study by the Defense Science Board[1] that the primary focus of a cyber force must remain the assurance of mission-essential functions (MEF) of the commander. Additionally, the distinction between intelligence (Title 50) and offense (Title 10) authorities notwithstanding, the proliferation of digital technology and the overlap between networks and computers blurred the traditional boundaries between offensive and defensive activities. Organizationally, the activation on 1 October 2009 of the US Cyber Command (USCYBERCOM) brought together computer network attack (CNA) and computer network defense (CND) activities of the Joint Functional Component Command for Network Warfare (JFCC-NW) and the Joint Task Force for Global Network Operations (JTF-GNO) under the USCYBERCOM. It is in this environment that the USAF vision of global vigilance, global reach, and global power across the full spectrum of conflict from peacetime to major combat operations drives the science and technology (S&T) requirements for cyber operations, as well as the educational requirements for cyber force development. Essential to USAF cyber forces is an organizing construct with a primary responsibility for assuring the USAF mission-essential functions in a contested cyber environment and a deployed responsibility to the joint force commander (JFC) through an expeditionary framework. However, properly educating that force of cyber warriors is a prerequisite.

Cyber Support to the USAF Vision

Rapid technology advances over the past three decades and the proliferation of computers into weapon systems created a dichotomy of net-centric military superiority and a commensurate reliance on vulnerable technology. The simultaneous depletion of the US computer industrial base and its

---

Dr. Kamal Jabbour, Scientific and Professional (ST), serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology, for the AF Research Laboratory, Rome, New York. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to Air Force organizations, the DoD, other government agencies, universities, and industry.

migration overseas reduced further the cost of net-centricity and increased disproportionately military dependence on foreign technology. Budgetary pressures compounded the slide away from assured government off-the-shelf (GOTS) stand-alone weapons towards affordable commercial off-the-shelf (COTS) networked systems.

Given this climate of rapid technological advance and global political change, the USAF recognizes the duality of cyberspace as a war-fighting domain as well as a foundational domain. As a war-fighting domain, cyberspace affords irregular adversaries a low-cost option to attack our global interests. As a foundational domain, cyberspace offers our peers an attack vector to negate our superiority in the traditional domains of land, sea, air, and space.

By adding cyberspace to its mission statement and standing up a cyberspace command, the USAF took on the challenge to develop and present forces ready to fight in this domain. This recognition of cyber warfare as a revolution in military affairs (RMA) raises fundamental questions on concepts, organization, and technology. Amidst these questions lies the challenge of presenting cyber options to the National Command Authority (NCA) and cyber-ready forces to the combatant commanders.

Whether or not Julius Caesar influenced the US Air Force vision of "Global Vigilance, Global Reach, Global Power" with his "Veni, Vidi, Vici" message to the Roman senate in 47 BC does not negate the evidence that these three tenets of warfare transcend time and technology. Two millennia later, the USAF S&T strategic vectors embody the Roman tenets and provide a road map to the USAF vision by (1) offering persistent situational awareness (SA), (2) delivering precision effects, and (3) providing access and survival in the battlespace. The changing mix of vigilance, reach, and power as tensions escalate toward major combat operations requires that cyber operations provide a necessary enabler for air and space power while providing an additional domain for delivering effects.[2]

Global Vigilance

Global vigilance is the ability to keep an unblinking eye on any entity—to provide warning on capabilities and intentions as well as identify needs and opportunities. The primary challenges of global vigilance include maintaining persistent, global, multi-domain SA using assured, trusted systems that can avoid a broad spectrum of threats. In turn, global vigilance depends to some extent on elements of global reach to support sensor positioning and forward basing of assets for SA. We identify situational awareness,

assurance and trust, and threat avoidance as the three main capabilities necessary to achieve global vigilance in and through cyberspace.

Mica Endsley defines situational awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[3] An objective of cyber SA is to provide automated situation assessment and analysis that meets the operational requirements of all areas within the cyber domain—friendly blue networks, traversal gray networks or global commons, and adversary red networks—across the entire spectrum of conflict. Mission awareness lies at the heart of situational awareness. Understanding the dependence of missions on specific assets, the interdependence of assets, and the interdependence of missions drives the requirements for SA.

Assuring missions and information and trusting systems and data provide the foundation for global vigilance across the spectrum of conflict. DoD Directive 3020.40, *Defense Critical Infrastructure Program*, defines mission assurance (MA) as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan." Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations*, defines information assurance (IA) as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation." Trust in a system requires trusting its hardware and software to maintain the integrity of data at rest and in motion as systems evolve in capability and technology.

Avoiding a threat through deterrence, domain modification, or agility provides a strategic defensive strategy that can reduce or eliminate the need to fight that threat. Effective cyber deterrence requires either a credible threat of retaliation with timely detection and attribution of attacks or a disincentive by increasing the cost of an attack and lowering its perceived benefits. Modifying the cyberspace domain to eliminate vulnerabilities or make them inaccessible to an adversary through sound hardware and software development practices can eliminate beforehand vulnerabilities by designing them out of a system. Agility includes establishing indications and warnings (I&W) mechanisms that detect anomalous activities or entities, rapid analysis of the activity to include attribution and geo-location, anticipation of future behaviors and effects, and effective real-time provisioning of defensive measures.

Global Reach

Global reach is the ability to move, supply, and position assets with unrivaled velocity and precision anywhere. The concepts that support global reach in cyberspace include access technologies to position and deploy cyber assets, survival in a contested cyber environment, and cross-domain superiority for command and control of integrated mission execution. Global reach encompasses the predominantly defensive measures of access, survival, and cross-domain operations. When a situation escalates from peace towards conflict, these measures enable the capabilities that support global power for major combat operations.

In all domains of land, sea, air, space, and cyberspace, access refers to deploying and positioning friendly forces across blue, gray, and red spaces. While traditional domains are fixed in size—the amount of available land, sea, air, and orbital space is essentially constant—the cyberspace domain changes dynamically and increases indefinitely in size and shape, creating unique technical challenges for the positioning of cyber assets.

An effective defense in depth avoids the majority of threats and defeats those threats that turn into attacks. When an attack evades detection and defeat and disrupts US systems and networks, the defensive priority turns to survival and mission assurance. In this context, MA seeks to ensure that critical MEFs fight through and recover from attacks against the underlying cyber infrastructure. Mission-aware systems that control dynamically end-to-end resources for IA-enabled mission assurance adapt to failures and attacks by reconfiguring resources to provide an acceptable level of service and security.

Cross-domain operations are another issue. In Internet terminology, a domain refers to a group of computers or IP addresses that share higher-order addressing bits or higher-order naming convention, while computer security terminology calls cross-domain operations those transactions that occur across different classification levels or across Internet domains at the same classification. We maintain consistency with the joint definition of domains as they pertain to war-fighting domains, and we use the term *cross-domain* to represent operations across land, sea, air, space, and cyberspace. Robust modeling and simulation and realistic war gaming permit experimental predeployment prototyping and evaluation of cross-domain effects, including the integrated delivery of effects from blue and red systems in every domain against red and blue systems in every domain. Integrated planning requirements for cyber assets mirror those for traditional intelligence, surveillance, and reconnaissance (ISR) and combat assets, yet the practice of procedural versus positive control

over air assets and the time scales of the air operations center (AOC) do not translate well to cyberspace, where decision cycles hover around a fraction of a second.[4] Cross-domain command and control enables cross-domain superiority and the freedom of use of air, space, and cyberspace, leading ultimately to cross-domain dominance and the freedom to attack and the freedom from attack in and through air, space, and cyberspace.[5]

Global Power

Global power is the ability to hold at risk or strike any target, anywhere, and project swift, frequently decisive, precise effects. Delivery of global power in any war-fighting domain requires command and control of cyberspace, on which modern US military capability depends. The global projection of cyber power to complement or enable kinetic power creates S&T challenges of developing precise cyber effects; estimating first-, second-, and higher-order effects; and taking response actions to external events.

Precision effects are the intended outcomes of offensive operations in any war-fighting domain. With conventional kinetic weapons, precision effects became synonymous with low collateral damage, given the maturity of tools and techniques for measuring the effectiveness of munitions. In measuring the effects of cyber operations, operators rely on intuitive estimates of effectiveness that depend in large part on the experience and expertise of the operator. Cyberspace operations can produce robust strategic, operational, and tactical effects across the entire spectrum of conflict. Second- and higher-order effects of cyberspace operations may extend beyond the immediate effects on a specific system necessitating a clear understanding of sustained cyberspace operations. Cyberspace operations can also create effects in other domains, enabling cross-domain effects delivery based on a cyber effects-based assessment (EBA).

Cyber EBA refers to the process that provides the war fighter with measured effects that quantify the outcome of a cyber operation into tactical, operational, and strategic impact. This process must occur in near real time during the prosecution of a mission by fusing multiple sensors and combining multiple means of measuring effects. This process must determine first-, second-, and higher-order effects on systems and on users while providing a side benefit of cyber EBA of kinetic operations. At the same time, cyber professionals must consider response action plans.

Computer network defense response action (CND-RA) refers to actions taken in cyberspace to defend blue forces against adversary attack. These

response actions must take place in real time during the prosecution of a cyber mission and must include response action for attack containment as well as offensive response action. The greatest complement to cyber vision support to global vigilance, reach, and power is a well-organized, well-educated cyber officer corps.

Organizing and Building an Initial Cyber Force

Assuring the mission of the USAF in a contested cyber domain remains the top priority of a USAF cyber force. Activating the Twenty-fourth Air Force under Air Force Space Command brings to the forefront the question of presenting cyber forces to the JFC. An expeditionary framework gives cyber officers a hands-on understanding of the threat through a joint force assignment and permits them to bring back to their mission assurance jobs a heightened appreciation for the risk trade-space between threats and vulnerabilities. To expedite this, the USAF must establish an expeditionary deployment schedule for the current cyber force in support of joint force commanders.

A centrally-managed, locally-commanded cyber force whose primary function is to assure essential functions of the various USAF commands is required. These extended periods of MA support include training on the latest tools, threat situational awareness, and the pursuit of graduate academic degrees, while exercising defensive measures to secure local cyberspace and the mission it supports.

Role and Responsibilities

A foundational principle of unity of command maintains that the success of a mission remains ultimately the responsibility of the commander. Therefore the USAF must delegate to local commanders the responsibility for assuring that piece of cyberspace on which their missions depend.

Recent air, sea, and space mishaps bring into focus the question of responsibility. The collision between two vessels may have resulted from the lack of timely SA. The crash of a remotely piloted aircraft (RPA) may have resulted from a dropped communication link. The aborted launch of a satellite may have resulted from indications of a mechanical malfunction. In all cases, cyberspace played the dual role of communicating SA to commanders and carrying back command and control instructions representing their intent. Under no circumstance can the responsibility for mission assurance shift away from the mission commander to a JFC responsible for securing the network—a piece of the cyber domain that enables the mission.

While a case may be made that JFCs must maintain command authority of offensive cyber forces operating under Title 10 authority in their area of responsibility (AOR), an equally compelling argument can be made that assuring a critical function in a contested cyber domain remains the responsibility of the MEF commander. Centralized command by a JFC of the cyber assets that enable essential cyber functions and the cyber forces that assure them creates an enormous challenge of understanding the complexity of every MEF and its dependence on cyberspace to the same fidelity as a local mission commander.

The central authority of a JFC or a USAF cyber command must extend only to the gateway of the critical systems that support individual essential functions. Thus, the computers and networks aboard a ship or an aircraft remain the responsibility of the platform commander, and those of a critical MEF remain the responsibility of the cyber MEF commander.

The present stance in favor of central management of cyberspace assets argues that a vulnerability in one system is a liability to all. By equipping MEF commanders with cyber officers educated to assure these functions in a contested cyber domain and delegating to those commanders responsibility and accountability for those cyberspace assets under their control, the cyber risk assumed by all becomes comparable to the risk of fratricide in conventional warfare. All services—Army, Navy, Marines, and Air Force—operate aircraft in the air domain and use elaborate deconfliction measures to minimize fratricide. Similarly, in cyberspace we must develop deconfliction procedures to enable MEF autonomy while minimizing the shared risk of fratricide.

Organizing the cyber force begins with a long-term strategy to develop cyber officers complemented with a stop-gap initiative to secure the USAF mission and present forces to the JFC. Currently, the Air Force does not have an adequate cadre of appropriately educated officers performing the cyber mission. Although they constitute only 7 percent of USAF officers, computer engineering (CE) and electrical engineering (EE) degree holders provide a solid foundation for the initial cyber officer corps. The USAF should recruit nonrated company-grade officers with CE and EE degrees for development into cyber officers through advanced graduate education and specialized DoD organic training. Replicating the success of the recent effort to recruit nonrated CGOs into RPA pilot-training slots, the Air Force should also invite young officers with technical degrees to apply for initial qualification as cyber officers.

As the Air Force builds an initial cadre of cyber officers, it must keep sight of their primary function—to assure the mission of the USAF in

a contested cyber domain. Upon completing graduate education, cyber officers must lead the task of mapping the dependence of critical MEFs on cyber systems to give commanders a first line of defense against cyber attacks. For the long term, however, the Air Force must commit to deliberately educating its cyber leaders.

Educating Cyber Officers

Educating cyber officers on the fundamentals of cyber operations leads to the development of a cyber force capable of dominating cyberspace across the entire spectrum of conflict. In his book *Strategic Warfare in Cyberspace*, Dr. Gregory Rattray contrasted the World War II strategic bombardment RMA to the current cyber warfare RMA.[6] He attributed the success of the former to a technology-enabled, industry-driven superiority and predicated the success of the latter on an education-enabled, technology-driven framework. The USAF vision of global vigilance, global reach, and global power provides the doctrinal foundation for the S&T of cyber warfare, while an S&T foundation provides the educational framework for cyber warfare.

Preparing forces for cyber warfare mandates distinguishing between education and training, a distinction one can ignore only at great peril. Training provides Airmen with proficiency to operate current tools, whereas education builds a foundation that prepares officers to deal with uncertain future challenges.

Delivering military options in cyberspace requires an elite, educated cyber officer corps augmented with a well-trained cyber force. A balance between educated strategic thinkers and trained tactical operators ensures the ability to fight in cyberspace across the entire spectrum of conflict. When educating a new breed of cyber officers, it is imperative to educate first on the science of information assurance and then train on the art of cyber operations.

An examination of Air Force Personnel Center records reveals an alarming drop in the number of engineers and overall scientific qualifications of USAF officers. National trends exacerbate this shortage. The US technological advantage as a nation and the corresponding military superiority depend vitally on the ability to reverse this trend. Deliberate cyber force development gives the USAF an opportunity to lead the nation in growing engineers.

The scientific and mathematical complexity of computer and network systems, the critical dependence of USAF essential functions on their proper operation and the uncertain risk trade-space between threats and vulnerabilities mandate a relevant formal college education as the entry point into

a cyber force. At a minimum, cyber warriors must hold an accredited bachelor's degree in computer or electrical engineering. This foundation provides the prerequisite grounding in the immutable fundamentals of cyber operations and prepares cyber officers for the challenges of an uncertain future.

Several additional recommendations surface when considering how the USAF can best develop and educate the future cyber cadre. An undergraduate degree in engineering as a prerequisite for admission into undergraduate pilot training (UPT) provides a first-order effect of an increase in the number of officer candidates pursuing engineering degrees with the goal of securing pilot slots, increasing consequently the number of nonrated officers with engineering degrees. As engineer-pilots move out of cockpits and into command positions, the second-order effect is a more technical leadership educated to deal with the uncertain challenges of the technological age. Requiring an engineering degree as a prerequisite to UPT gives American youth an incentive to take more high school courses in mathematics and science and contributes to reversing the free-fall in the national academic standards in mathematics and science.

Additionally, the USAF is increasing the number of four-year full scholarships to top US programs in computer and electrical engineering. Targeting scholarships to a dozen premier institutions creates a class of young officers with shared experiences and allows the USAF to influence curriculum development to meet national requirements. A secondary effect of targeting selected schools is the inevitable growth in civilian demand for these programs and the resulting increase in an educated civilian cyber workforce equipped to augment DoD assets.

Designing the Cyber Curriculum

The complexity of electronic systems, their rapid incorporation into all facets of traditional warfare, and the uncertainty of future threats necessitate educating cyber officers on both timeless science and timely technology. The technical challenges form the basis of a balanced curriculum in cyber warfare education. The desired outcomes of this curriculum are (1) educating future cyber leaders on the science and technology of cyber warfare to prepare them to tackle the future challenges of a rapidly evolving domain, (2) providing them a solid grounding in the arts and sciences of a computer engineering foundation, and (3) developing them into cyber officers—Airmen, leaders, and warriors.

What follows is the philosophy underlying an orthogonal curriculum and the outline for a sample track leading to a bachelor of science (BS)

degree in cyber warfare. This representative curriculum recognizes physics and electrical engineering as the foundation for cyberspace, a domain characterized by the use of electronics and the electromagnetic spectrum and mathematics and computer science as the foundation for storing, modifying, and exchanging data via networked systems and associated physical infrastructures. Computer engineering, the center of gravity between electrical engineering and computer science, brings the theories underlying the domain into the practice of warfare.

The requirements of a four-year BS degree in computer engineering are the cornerstone of cyber education and incorporate an eight-semester track on cyber warfare. The formal academic framework necessary to tackle the technical challenges in cyber warfare extends across a continuous spectrum from mathematics, computer science, computer engineering, electrical engineering, and physics, as shown in the figure below.[7]

Foundation continuum for cyber education

The primary goal of this cyber officer development plan is to create cyber officers who comprehend the concept of cyber as a revolution in military affairs. This concept seeks to instill an appreciation of the uniqueness of cyberspace as a war-fighting domain—the third domain for the Air Force after air and space—as well as a foundational domain vital to land, sea, air, and space operations. It teaches an appreciation of the broad range of functions and capabilities in cyberspace and differentiates between the limited scope of network operations and the pervasive scope of cyber warfare.

Cyber Warfare Curriculum

We divide the curriculum content for developing cyber warriors into a four-year course of study including fundamentals in the freshman year, tactical in the sophomore year, operational in the junior year, and strategic in the senior year. A typical CE curriculum permits the addition of the cyber warfare component as a concentration with minimal impact on accreditation. In fact, during the last two years, cyber courses can replace certain programming and system design courses while focusing the capstone design project on cyberspace. Alternately, cyber security electives or service-specific instruction may replace the AF-centric strategic cyber warfare component.

Some of the topic areas presented as fundamentals include computer systems, information operations doctrine, cryptography, network architecture,

and computer network operations. During the second year, candidates study access to adversary systems, stealth and persistence, cyber effects, cyber intelligence, and steganography. Year three introduces access control methods, secure network operations, cyber SA, digital forensics, high-assurance programming, and mission assurance. In the last year, students tackle problems concerning national security and military strategy, warfare in cyberspace, strategic effects of cyber war, challenges and constraints of cyber options, employing cyber options as a campaign plan, and cyber anticipation and adaptation. Throughout the course of study, cyber laboratories support experiential learning and greater appreciation for cyber capabilities.

The age of cyber is upon us, and the USAF has a vested interest in organizing a cyber force to meet the challenges of the age while supporting the current vision of global vigilance, reach, and power. This challenge requires an organizing structure with expeditionary features, clear lines of authority, responsibility, and unity of command backed up by deliberately educated cyber leaders. Air Force cyber leadership presents a historic opportunity to put the nation on a correct vector to secure cyberspace and to help assure the national mission-essential functions that depend on it. SSQ

Notes

1. Defense Science Board, *Challenges to Military Operations in Support of U.S. Interests: Report of the 2007 Summer Study* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, December 2008).
2. Kamal T. Jabbour, "The Science and Technology of Cyber Operations," *High Frontier Journal* 5, no. 3 (May 2009).
3. Mica R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 (1995): 32–64.
4. Procedural control—a method of airspace control that relies on a combination of previously agreed and promulgated orders and procedures (JP 3-01, *Joint Doctrine for Countering Air and Missile Threats*). Positive control—a method of airspace control that relies on positive identification, tracking, and direction of aircraft within an airspace conducted with electronic means by an agency having the authority and responsibility therein.
5. The Strategic Studies Group at Checkmate said, "We believe superiority represents freedom to act, but dominance includes the ability to exploit." This implies that dominance exceeds superiority. However, referencing the definition of air superiority from JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*: "air superiority—That degree of dominance in the air battle of one force over another that permits the conduct of operations by the former and its related land, sea, and air forces at a given time and place without prohibitive interference by the opposing forces," superiority is a degree of dominance. Excerpts from Cross-Domain Dominance brief by Lt Col Brad "Detroit" Lyons and Lt Col Tim "Dexter" Rapp, AF Strategic Studies Group, Project Checkmate, 10 June 2008.
6. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Boston: MIT Press, 2001).
7. For additional information, including detailed charts listing the complete four-year curriculum requirements for cyber development, contact the author, Kamal.Jabbour@rl.af.mil.