Cyber Operations
Bridging from Concept to Cyber Superiority

By JAN KALLBERG *and* BHAVANI THURAISINGHAM

U.S. Air Force (Daniel J. Rohan, Jr.)

Chief of Cyber Defense Center for Brazilian army participates in international cyber collaboration panel at 2011 U.S. Strategic Command Cyber and Space Symposium

The United States is preparing for cyber conflicts and ushering in a new era for national security. The concept of cyber operations is rapidly developing, and the time has come to transpose the conceptual heights to a broad ability to fight a strategic cyber conflict and defend the Nation in a cohesive way. Richard M. George, a former National Security Agency official, commented on recent developments: "Other countries are preparing for a cyberwar. If we're not pushing the envelope in cyber, somebody else will."[1] Therefore, increased budgets are allocated to cyber operations research and education. The Defense Advanced Research Projects Agency (DARPA) Plan X (for which a formal solicitation has not yet been issued at the point of authorship) will, according to media outlets, give an additional infusion of $110 million to research in pursuit of cyber operational capacities. Herbert S. Lin of the National Research Council of the National Academy of Sciences commented, "They're talking about being able to dominate the digital battlefield just like they do the traditional battlefield."[2] Plan X adds to the DARPA budget of $1.54 billion for cyber research in the period 2013–2017.[3] Additional funds are allocated for a variety of Federal agencies.

The most desirable goal is to acquire cyber supremacy—global U.S. dominance in cyberspace that permits the secure, reliable conduct of operations by U.S. forces and related land, sea, air, and space forces at a given time and sphere of operations without prohibitive interference by an adversary.[4]

Universities are instrumental in bridging from concept to methodology, tools, and implementation. They are the force multiplier of the cyber defense doctrine as research hubs, educating thousands in the civilian and military-contractor workforces, and as a provider of technical solutions to ensure mission success. It is pivotal for cyber superiority that institutions of higher learning are aligned with the strategic goals of our national cyber defense strategy and clearly understand its doctrinal underpinnings. Put differently, if cyber security research is driving in a different direction than the national cyber strategy, we are getting in trouble by creating a gap and a weakness that can be exploited by hostile parties. Not only do we lose the opportunity to acquire cyber superiority, but we also become the prey in cyberwar.

This article challenges the universities' abilities to provide support for the doctrinal change to cyber operations, mainly because of the overemphasis on information assurance and the lack of intra-university collaboration.[5] Another issue considered is that in case we fail to transpose the theory to broad implementation, adversaries may be watching and learning what we should be implementing. The support for this scenario is drawn from the development of armored warfare.

The Business of Information Security

Traditionally, information security research and education have been founded on the key concept of *information assurance*—actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. Information assurance is often expressed in underlying subfields such as forensics, network security, and penetration

Dr. Jan Kallberg is a Research Associate in the Cyber Security Research and Education Center in the Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas. Dr. Bhavani Thuraisingham is the Louis A. Beecher Jr. I Distinguished Professor in the Department of Computer Science and Executive Director of the Cyber Security Research and Education Center.

testing. It is similar to positional warfare displayed at the Western Front of World War I. The front would be quiet for a long period, then an attack would erupt in heavy bombardment followed by an attempt to penetrate the defense lines, and the key to victory would be to hold a few heavily fortified positions in a battle of attrition.

In information security, victory has included providing for restoration of information systems by incorporating detection, protective, and reactive capabilities. Restoration is similar to recapturing a lost trench, to use terminology from trench warfare. The defensive posture has been reflected in research, research funding, and scholarly output. From information security's early inception in the 1980s to today's secured environments, we have become skilled in our ability to secure and harden information systems. The fluid and soon-to-be-automated battlefield of cyber operations is a novelty. The defense and intelligence establishments are moving quickly toward full-spectrum cyber operations.[6] The challenge for cyber security research centers is to adapt to the changing environment as the earlier academic paradigm assumption of future conflict is invalidated.

The Lure of Traditional Thinking

The cyber warfare concepts and abilities of the early years will continue to evolve over the decades to come. Developments tend to take longer than first anticipated not only because of technological hindrances, but also due to a path-dependent culture favoring earlier methods and a natural instinct to prefer what is known. There is a valid analogy between the dawn of cyber warfare and the dawn of armored warfare. It took 25 years for Western armies to figure out a proper use for the armored tank. Once that was understood, the way wars were fought was fundamentally changed. That has continued for 70 years and still counting.

For the first 25 years, the French and British saw the battle tank as a moveable machinegun pillbox from trench warfare. The tank was not a fighting platform; it was a mobile fortification that supported infantry. This perception changed when those countries suffered a horrifying defeat to the Germans in May 1940; the Germans had studied, developed, and understood armored warfare. For the Allied forces, it was too late; the damage was done. The irony is not only that the French developed many of the ideas the Germans utilized, such as Charles de Gaulle's proposed armored warfare tactics and the French airmen's innovation of advanced dive-bombing, but also that the Allies publically and vocally debated the opportunities these tactical innovations offered. The Germans were listening, but not the Allied high command. Due to groupthink and intellectual path dependency, the French military never accepted it or even considered it seriously.

The French preferred structured positional warfare. An integral part of positional warfare was fighting for fixed hardened positions—a war of holding positions and attrition. In 1940, France had the largest land army and also the largest number of battle tanks in Western Europe. In addition, there were Allied forces such as the British Expeditionary Force.

The difference between the combatants was the tactics of how to use battle tanks. The German strategy—which was old and known to the French—was an attempt to encircle the French after a breakthrough, but the tactics and operational performance were revolutionary. The German tanks were in the hands of Heinz Guderian, who carefully studied how to utilize tanks in an unconventional manner. He invented and refined armored warfare, ensuring that he could exploit the adversary's weaknesses. The number of French tanks and massive French army did not matter. The reason was simple: the French were not able in their minds to fight modern warfare and therefore were doomed to destruction or submission.

Guderian utilized the embedded abilities of armored units. The Germans changed the aim point, and instead of racing toward Paris through Belgium, the armored units pushed toward the Atlantic Coast to cut off the Allied forces in Flanders and Belgium where they waited for a repeat of the attack of 1914. The Sichelschnitt Plan of 1940 was designed for armored warfare; it had momentum and speed and captured the initiative. Once executed by the Germans, the French line of defense collapsed. After the Blitzkrieg of 1940, Guderian wrote about his preparation:

For someone observing tank theory from afar, unburdened by tradition, there were lessons to be learned in the employment, organization and construction of armor and of armored units that went beyond the doctrines then accepted abroad. After years of hard struggle, I had succeeded in putting my theories into practice before the other armies had arrived at the same conclusions. The advance we had made in the organization and employment of tanks was the primary factor on which my belief in our forthcoming success was based.[7]

The opportunity in cyber operations in the next decade is not a revolutionary technology, but instead derives from how we utilize and militarize existing technologies in a way that is unburdened by tradition, to use Guderian's words.

The French in 1940 were still thinking of warfare as a solid front between two adversaries, consisting of three lines of units: infantry, artillery, and bakery. The traditional way of fighting war was that infantry faced and fought the enemy, artillery supported the infantry with indirect fire, and the rear echelon, here called bakery, provided logistic support. Guderian broke the rules and fought the war in reverse order. He concentrated his units and overran the French lines at a weak point, and in a deep stroke attacked the bakery, ignored the infantry, and let the artillery panic. The attack was identical to the sketches of deep-penetrating armored assaults that Liddell Hart and de Gaulle envisioned before the war.

The lure in applying traditional military thinking on cyber warfare is that we can fight cyberwar based on the doctrines and intellectual underpinnings of land battle as we know it. Carl von Clausewitz assumed that the soil, woods, heights, and rivers of the Napoleonic battlefield were fixed. In a Clausewitzian world, the battle commander could understand and study the battlefield, and by objective permanence, the intended battlefield would be there the next day ready for battle. The woods would not move, the rivers would not disappear, and the heights would not sink. In cyber, the map and terrain that form the battlespace change continuously in real time and beyond our imagination as new nodes are discovered and a kaleidoscope of network patterns occurs and disappears.

the defense and intelligence establishments are moving quickly toward full-spectrum cyber operations

Traditional military theories could be less relevant in cyberspace than we are ready to admit. Traditional thinking appeals to us, but it could be spurious.

If we assume that we have control of the situation and knowledge of our enemy's positions and the full extent of the map, with our defense focused on hardened strongpoints, then we are fighting the digital cyberwar with the tools of analogue positional warfare. Edward N. Luttwak noted that strategy only matters if we have the resources to execute the strategy, and embedded in Luttwak's statement is the general condition that if we are unable to identify, understand, and utilize our resources, strategy does not matter.

Cyber supremacy will be achieved if we can understand the unique tenets of cyber, create a doctrine that exploits opportunity and technical ability, achieve broad societal alignment to cyber strategy, and assemble the workforce to execute it. Universities play a vital part in the last three components. Even if the military develops the brightest and most thought-through doctrine ever conceived, it will still be only a doctrine and nothing more. Doctrines are instruments of war, but they tell only how to play the cards; the actual deck of cards in cyberwar is mainly produced by private enterprises and academia.

Inability to Transpose Theory to Practice

The United States is having an extensive public debate about the future of cyber warfare and how it should be conducted. We debate openly as a free and democratic society. We are not the first open society that has been able to generate magnificent ideas and theories about future warfare. In the 1930s, B.H. Liddell Hart, Giffard Le Quesne Martel, and John F.C. Fuller wrote extensively about the future of mobile warfare. Martel was considered one of the world's leading tank experts of the 1930s. He went so far to prove his case that he built a light tank in his own garden, at his own expense, which became the platform for the British Bren gun-carrier.[8] Liddell Hart was a prolific writer and developed theories of exploits after an armored breakthrough of enemy lines, the deep strike that would force the enemy to react and lead to the collapse of the defense. In France, then–Colonel Charles de Gaulle advocated for armored divisions, freeing the tank corps from the infantry and utilizing armored warfare's full potential. France and Britain in the 1930s saw the potential in armored warfare, but for institutional reasons and internal biasness, they refused to capitalize on these modern ideas.

In the 1930s, both France and Britain failed to transpose theory to methods, tools, and implementation. In military terms, theory transposes to tactics, weapons, and training. Theory was created in France and Britain but transposed by Germany through generals such as Erich von Manstein and Guderian to tactics, weapons, and training. Guderian wrote after the war: "The proposals of de Gaulle, Daladier and others along these lines had been ignored. From this it must be concluded that the highest French leadership either would not or could not grasp the significance of the tank in mobile warfare."[9]

even if the military develops the most thought-through doctrine ever conceived, it will still be only a doctrine

The United States faces the same risk as Britain and France in the 1930s, except our military leadership clearly understands the changing paradigm; there are other obstacles to transposing theory. We are the creators of cyber ideas and concepts, but we fail to move beyond the present and implement them. Today, the Department of Defense (DOD) and Intelligence Community are world leaders in developing cyber operation concepts and innovative strategies to ensure future American cyber supremacy. Instead of the military being the blockage for intellectual proliferation as it was in France 75 years ago, the hindrance for cyber warfare's development today is in the civil society and the academic realm.

We can assume that our adversaries or covert adversaries in the digital age carefully study our new strategies and ideas and develop plans to utilize these publically discussed innovative concepts. The most loyal online readers of the offensive cyber operation discourse in American journals are likely our adversaries. All of them are ready to capitalize on our ideas if they can.

The University Role in Cyberwar

A nation's cyber warfighting ability will be determined by its ability to mobilize resources and knowledge and coordinate the effort. These resources are not as easily identified. At the entrance to the contested cyberspace as a warfighting domain, academia and university research centers have to find their new roles. University cyber researchers have continued to deliver mainly information assurance. Even the information assurance context has been following the Zeitgeist by focusing on Cold War spies, terrorists, drug cartels, white-collar crime, and economic espionage. The bottom line is that it is still information security with a theoretical foundation from the 1980s. Information security has had a decade of high levels of funding as a response to 9/11 and society's increased reliance on the Internet and computerized systems. This posture has been built on hardening systems. The surge of resources to research centers, contractors, Federal agencies, and private industry has resulted in a greater understanding of how to secure systems.

Basic operational questions as to why things are done, their strategic value, how they can tangibly strengthen operations, and the factual effects have sometimes been overshadowed by details with limited systematic thinking behind them. Traditional information security—the hardening of systems—has been so prevailing that it is often misinterpreted as exchangeable with cyber defense and cyber operations.

In the pursuit of cyber superiority, information security, renamed information assurance, is one piece among many and, depending on the operational environment in different scenarios, is of even less importance than other measures. DOD defines *cyber superiority* as "the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations of that force, and its related land, air, sea, and space forces at a given time and sphere of operations without prohibitive interference by an adversary."[10] Dominance in cyber space can only be achieved if there is an ability to collect information, attack and intercept other actors' cyber activities thus preventing their interference, and likely also utilizing digital lethality to destroy or severely damage other actors' cyber systems. Information assurance is not enough. It is part of cyber defense—but it is not cyber defense.

The National Security Agency (NSA) has set up criteria for the designation of academic departments as Centers of Academic Excellence (CAE) to ensure that the quality of education and research is upheld. There are 48 research centers and university departments

that have been considered Centers of Academic Excellence–Research (CAE-R). NSA's latest addition is CAE Cyber Operations.[11] According to the NSA, key abilities are collection, exploitation, and response. The majority of the CAE-R institutions are likely to pursue the CAE Cyber Operations.

A Quick Survey

As an experiment, we conducted a survey to get a snapshot of where CAE-R research centers stand today in relation to the broader systematic full-spectrum view on cyber warfare pursuing cyber superiority. The question was whether the academic institutions are embracing the cyber operations paradigm shift or are institutionally path-dependent and continuing with the information assurance track that has been prevailing since the Cold War. The purpose of the survey was to determine how many research universities have broken down their internal walls between departments in professional and engineering schools and successfully pursued a broader approach to match the complexity of cyber operations. We acknowledge that this paradigm shift is a work in progress, and we have credited schools that are moving toward cyber operations even if the actual approach as of today is ad hoc and less defined.

Cyber operations research requires linkages outside of the engineering schools and benefits from collaboration with other university-wide schools and departments. The research can then be transferred through research-based education to the workforce that is needed to achieve national cyber defense objectives. A broader knowledge base enables the research center to do work that can support, prepare, and conduct defensive countercyber operations, offensive cyber operations, and cyber operational preparation of the environment aligned with the national interest.

A set of variables was created and then each academic CAE-R research center's Web presence was visited, along with their leading researchers' Web presence, and the materials presented on the Web site were evaluated against the variables. Some of the observations were reviewed and validated by an external reviewer to ensure that the evaluation did not contain systematic errors. There were 48 academic cyber research centers in nonmilitary higher education in the United States in February 2012. All schools that met the CAE-R criteria had information assurance programs in place as the foundation for the designation. The variables used were:

- whether there is research on offensive and responding cyber defense and if the research conducted steers toward offensive countercyber, cyber operational preparation of the environment, and pursuing cyber superiority in cyber warfare, or is predominantly based on information assurance only
- if there is a legal component supporting utilization of weapons control status, especially international law, ethics, and privacy, and a future need for assessments of military ethics, cyber rules of engagement, and the legal foundation for collateral effects, first and second tier
- whether the research has involved political scientists or other social scientists, especially in theories about national institutional stability and international relations, creating understanding of foreign societies or institutions that are the targeted adversaries, aligned with the concept of cyber operational preparation of the environment and information operations, leading to increased effect on adversarial society

U.S. Navy (Robert Wood, Sr.)

Commander of U.S. Fleet Cyber Command speaks to Information Dominance Corps Sailors at Naval Station Mayport, Florida

■ if the university has a designed policy school or similar entity to determine the extent of resources available on campus to optimize cyber operations research to take advantage of intelligence-gathering opportunities, human terrain, political instability, and fragile institutional design of target countries or institutions

■ whether there is a clear linkage between the cyber research program and policy school of the same university, if one exists

■ if security studies scholars are involved in the cyber security research, creating an understanding of security fundamentals and military science that would support a better understanding of the final goal with the cyber operation mission and doctrinal goals

■ whether there is an international relations component in the research to determine the degree the opportunity to exploit human terrain, political instability, and fragile institutional design of target countries or institutions is understood

■ if the cyber research covers the space domain since the importance of the defense of the global information grid is clearly identified by the term *cyber operations*, defined as the "employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[12]

Cyber attacking U.S. space assets can give high returns for an adversary.[13] The global information grid is pivotal to U.S. military might and information supremacy.[14]

Results and Reflections

We do not consider this survey as delivering a perfect picture of the state of national cyber research, but it will reveal a fundamental understanding of what research universities are able to deliver and where the majority of the U.S. cyber security research centers are on the learning curve. All 48 CAE-Rs are researching information assurance. Only five are actively researching offensive and defensive cyber operations to a broader extent. This includes research supporting information operations and psychological operations aligned with future military operations. If a military commander wants to have cyber weapons made, these universities are able to make military grade cyber weapons.

The high number of CAE-Rs that have legal components in their research reflects privacy research, which is also an integral part of information assurance. Only 10 CAE-Rs involve social scientists in their research. A significant number of schools do not involve social scientists in projects that are focused on human behavior and institutional arrangements. A few universities go as far as to design complex research projects that are partly based on behavior, sociopolitical institutions, and societal factors with only computer scientists and engineers on the team. Of the 48 CAE-Rs, 10 have a full-size policy school on campus, with numerous specialized scholars running research over a spectrum of policy related inquiries and with understanding of core tenets of societal cyber operation components. Only 5 CAE-Rs out of these 10 collaborate to a visible degree with their own policy school and utilize the joint knowledge. In other terms, half of the tier-one universities with cyber security research centers underutilize their own policy schools' pool of competence. Even if we are in a globalized world with cyber as not only a warfighting domain, but also an arena for international cybercrime and transnational illicit activities, only 6 CAE-Rs involved international relations scholars in their projects. Cyber issues in space only draw interest from 5 CAE-Rs.

The largest portion of the CAE-R cyber research centers is doing information assurance research independently and separated from other scholarly activity on their

Survey Results of 48 Centers of Academic Excellence-Research (Defense Department Institutions Not Counted)

Variable	Number of schools	Percentage of total
Offensive cyber research, such as offensive countercyber and cyber operational preparation of the environment	5	10.4
Legal considerations and privacy	18	37.5
Involving social scientists and/or behavioral scientists	10	20.8
Policy school on campus	10	20.8
Utilizing the assets of a policy school	5	10.4
Presence of security studies scholars or activity in research	14	29.2
International relations	6	12.5
Cyber in outer space, considering outer space as a part of cyber defense	5	10.4

campuses. The results are presented in the accompanying table.

Concerns and Opportunity

Cohesive cyber defense research requires universities to optimize their campus-wide resources to fuse knowledge, intellectual capacity, and practical skills in an unprecedented way. This is a major challenge for universities that have historically separated departments and schools and driven specialization so far that intra-university collaboration seldom occurs. In an era of austerity, it is justifiable for DOD to steer toward applied research that can strengthen the abilities of the Armed Forces and Intelligence Community and provide policymakers and Federal executives with more options.

the problem is that theoretical concepts do not become transposed into research and education to create methodologies, tools, and implementation

The future will require cyber defense research teams that can address not only computer science, electrical engineering, and software and hardware security, but also political theory, institutional theory, behavioral psychology, deterrence theory, military ethics, international law, international relations, and additional social sciences. Researchers working alongside DOD to develop tool sets for information operations as a subset of cyber operations, utilizing social media and exploiting collective behavior, would require a broad mix of social science and behavioral psychology competencies.

The problem, and our disadvantage, is that theoretical concepts do not become transposed into research and education to create methodologies, tools, and implementation. A vast number of our academic institutions are unable, as of today, to look at and conduct research beyond information security. Cyber operations require a different academic culture where collaboration in the national interest prevails over departmental turf wars. To quote Sayre's Law, "In any dispute the intensity of feeling is inversely proportional to the value of the stakes at issue"—and its corollary—"that is why academic politics are so bitter." A sense of what is ultimately at stake needs to be infused. Cyber research centers and dedicated researchers within different departments can be brought to an understanding of the need to collaborate, and they can even seek to collaborate, but the internal culture often prevails.

There could be several reasons why the academic turf war mentality exists. One is funding; cyber defense is seen as one of the few areas where funding could increase significantly in the future. Academic departments are trying to set out on their own journeys to seek sponsored research instead of jointly seeking grants with other disciplines, which would lead to fewer resources once they are shared.

For researchers, it is always more pleasant to be granted more money in the field we have already submerged ourselves in and fully understand. For researchers in general, it is also hard to admit that our little niche of science may not matter that much in the future. The academic community in many ways is driven to seeking more funding for what has interested researchers in the past rather than adapting to the new cyber paradigm, thus digging deeper trenches in the turf war.

A second reason the turf war exists is academic gridlock, which is a matter of institutional culture, intellectual path dependency, and the fact that many institutions became used to access to funding during what then–Secretary of Defense Robert Gates called an era of endless money. Once universities figured out the magic algorithm to get funding, the universities were less responsive to signals of change. If that predicted stream of funding disappears, action will be taken. The fastest way to correct the gridlock and increase the transformation of research and education to better mirror the interest of DOD is to steer funding. One of America's advantages in research is its universities' ability to quickly adapt when facing the risk of losing funding.

The conducted survey presents a misalignment between what is researched and educated in the Nation's cyber security research centers and DOD's overarching goals and doctrine. It has to be made clear that the stakes are so high that a correct balance has to trump any internal academic politics. The misalignment creates a gap that can be closed by steering funding and increasing interaction among the actors in the national cyber defense. Unless corrected, the misalignment will continue to create a national security risk. These innovative ideas can be put to use by our adversaries while we as a nation fail to achieve cyber superiority. **JFQ**

NOTES

[1] Ellen Nakashima, "With Plan X, Pentagon seeks to spread U.S. military might to cyberspace," *The Washington Post*, May 30, 2012, available at <www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html?hpid=z1>.

[2] Ellen Nakashima, "U.S. accelerating cyber-weapon research," *The Washington Post*, March 13, 2012, available at <www.washingtonpost.com/world/national-security/us-accelerating-cyber-weapon-research/2012/03/13/gIQAMRGVLS_story.html>.

[3] Nakashima, "With Plan X."

[4] Air Force Doctrine Document 3-12, *Cyberspace Operations* (Washington, DC: Headquarters Department of the Air Force, July 15, 2010, incorporating Change 1, November 30, 2011), 2.

[5] Jan Kallberg and Bhavani Thuraisingham, "Towards cyber operations—The new role of academic cyber security research and education," IEEE Intelligence and Security Informatics 2012, Washington, DC.

[6] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, available at <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=3&hp>; Evan Perez and Adam Entous, "FBI Probes Leaks on Iran Cyberattack," *The Wall Street Journal*, June 5, 2012.

[7] Heinz Guderian, *Panzer Leader* (New York: Dutton, 1952).

[8] Obituary of General Sir Giffard Martel, *The Glasgow Herald*, September 4, 1958, 9.

[9] Guderian.

[10] James E. Cartwright, memorandum, "Joint Terminology for Cyberspace Operations," Department of Defense, Washington, DC.

[11] National Security Agency, "Criteria for Measurement for CAE/Cyber Operations," available at <www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_criteria.shtml#4>.

[12] Cartwright.

[13] Jan Kallberg, "Designer Satellite Collisions from Covert Cyber War," *Strategic Studies Quarterly* (Spring 2012).

[14] William J. Lynn III, "A Military Strategy for the New Space Environment," *Washington Quarterly* 34, no. 3 (Summer 2011), 7–16.