REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAY 2009	Journal Article Postprint	May 2008 – May 2009

4. TITLE AND SUBTITLE
THE SCIENCE AND TECHNOLOGY OF CYBER OPERATIONS

5a. CONTRACT NUMBER
In-House

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62702F

6. AUTHOR(S)

Kamal Jabbour, Scott Adams, Mark Gorniak, Todd Humiston, Patrick Hurley, Herb Klumpe, Paul Ratazzi, Paul Repak, Brian Sessler, James Sidoran, Jason Siegfried, George Tadda, Walt Tirenin, Thomas Vestal

5d. PROJECT NUMBER
4519

5e. TASK NUMBER
PR

5f. WORK UNIT NUMBER
OJ

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AFRL/RIGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2009-55

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution unlimited PA# 88ABW-2009-0393 Date Cleared: 5 February 2009

13. SUPPLEMENTARY NOTES
Paper published in the Air Force Space Command Journal High Frontier, Volume 5, Number 3, May 2009, pp. 11-15.

14. ABSTRACT
The Air Force Research Laboratory provides the science and technology (S&T) vision, leadership, and products that enable the United States Air Force (USAF) to accomplish its mission to "fly, fight, and win in air, space, and cyberspace." The dependence on cyberspace of US weapon systems, critical infrastructure, financial institutions, and our way of life creates an imperative to operate freely in this domain. The USAF vision of global vigilance, global reach, and global power depends vitally on the ability to dominate cyberspace through integrated defensive and offensive operations across blue, red, and gray cyber systems, as well as across the global cyberspace commons. This article describes an S&T perspective on cyber operations within the focus necessary to operate in a contested cyber domain and to assure critical military missions in land, sea, air, and space against threats in cyberspace.

15. SUBJECT TERMS
Cyberspace; cyber operations; global vigilance; global reach; global power; situational awareness; assurance; threat avoidance; access; survival; cross-domain operations; effects; effects assessment; computer network defense response action

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			E. Paul Ratazzi
U	U	U	UU	6	19b. TELEPHONE NUMBER (*Include area code*) N/A

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Senior Leader Perspective

The Science and Technology of Cyber Operations

Dr. Kamal Jabbour, ST
Senior Scientist, Information Assurance
Air Force Research Laboratory, Information Directorate
Rome, New York

The Air Force Research Laboratory provides the science and technology (S&T) vision, leadership, and products that enable the United States Air Force (USAF) to accomplish its mission to "fly, fight, and win in air, space, and cyberspace." The dependence on cyberspace of US weapon systems, critical infrastructure, financial institutions, and our way of life creates an imperative to operate freely in this domain. The USAF vision of global vigilance, global reach, and global power depends vitally on the ability to dominate cyberspace through integrated defensive and offensive operations across blue, red, and gray cyber systems, as well as across the global cyberspace commons.

Joint Publication 1-02, Department of Defense (DoD) Dictionary of Military and Associated Terms, defines:

> **cyberspace** as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers *and* **cyberspace operations** as the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

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 S&T requirements for cyber operations. Figure 1 illustrates the changing requirements for vigilance, reach, and power as tensions escalate towards combat. Within this context, cyber operations provide a necessary enabler for air and space power, while providing an additional domain where the USAF can deliver effects.

The S&T requirements for cyber operations do not focus only on conducting operations in cyberspace, but rather look holistically at the cyber S&T necessary to accomplish the USAF vision of global vigilance, global reach, and global power in all three domains of air, space, and cyberspace.

Cyberspace is viewed first and foremost as a foundational domain that enables US military superiority, and secondarily as another domain where the US can deliver effects.

Through cross-domain dominance, operations in cyberspace can guarantee freedom of maneuver and assure mission essential functions (MEF) in all warfighting domains.

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.[1] The primary challenges of global vigilance include maintaining persistent, global, multi-domain situational awareness (SA) and 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 (1) SA, (2) assurance and trust, and (3) threat avoidance as the three main capabilities necessary to achieve global vigilance in and through cyberspace.

Situational Awareness

The strategic objective of cyber SA is to provide automated situation assessment and analysis that meet 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—from peacetime to major combat operations.

Mission awareness lies at the heart of SA. Understanding the dependence of missions on specific assets, the interdependence of assets and the interdependence of missions drives the requirements for SA.

Mica R. Endsley defines "SA 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."[2]

Perception: Perception represents the transformation of a signal into an alert. Significant technical progress on the perception of the elements of an environment appears in intrusion detection systems, vulnerability assessment, network mapping, configuration management, network management, and policy management. The real-time collection and long-term maintenance of meaningful data for blue, gray, and red systems present a fundamental technical challenge for perception.

Aggregation refers to correlation and fusion of raw data into activities of interest based on factual relationships or an implied requirement for additional meaning. The set of activities of interest at any point in time describe the current situation of the environment, and depend highly on the local environment. A technical challenge of aggregation is developing the appropriate situation at the appropriate level for the appropriate operator while maintaining consistency among differing views of similar

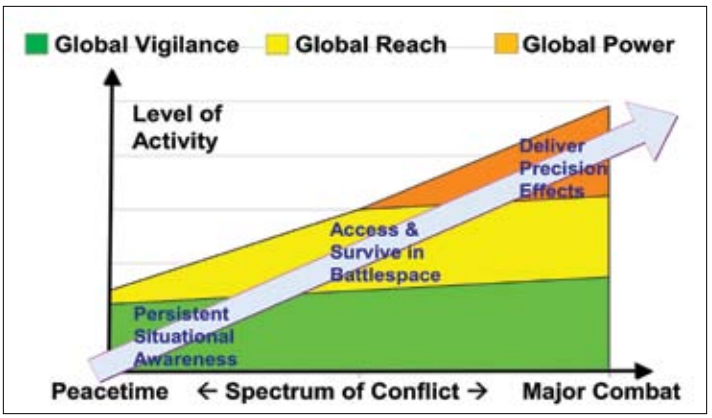

Figure 1. Level of activity across the spectrum of conflict.

situations.

Comprehension: The perception of activities of interest paves the way to their understanding and contextual placement into the environment and the comprehension of their meaning. Comprehension of meaning of a situation through assessment and analysis presents a significant technical challenge and an area of active research. Understanding a situation requires a broad range of analysis and an assessment of the impact of the situation on components, systems and missions.

Comprehension of meaning may require establishing additional relationships between activities of interest. Assessing the impact of an attack on a mission requires both attack activity and an activity that defines the relationship between MEFs and cyber assets that support those functions. The combination of these two activities can lead to deeper understanding of the impact of an attack on missions. Extending this analysis to hypothetical future situations allows reaction planning and response development.

Projection: The projection of status in the near future entails taking the current situation and analyzing plausible threats, opportunities, risks, and possible next steps. The path from the current situation to plausible future situations becomes the basis for developing courses of action (COAs) to move along a probable path and providing input into rules of engagement (ROEs).

The projection of status ranges from analyzing an attack graph to determining the existence of additional attack paths to discovering alternative solutions for fighting through an attack. Across this range of possible actions, the projection of a situation to plausible future situations presents a substantial technical challenge.

Assurance and Trust

Assuring mission and information, and trusting systems and data, provide the foundation for global vigilance across the spectrum of conflict.

Mission Assurance (MA): DoD Directive 3020.40 defines MA as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the National Military Strategy."

The principal responsibility of a commander is to assure mission execution in a timely manner. The reliance of MEFs on cyberspace makes cyberspace the target of choice for an adversary who cannot, or chooses not to, face us in conventional battle. To assure these MEFs in a contested cyber domain requires mapping MEF dependence on cyberspace, mission prioritization to ensure continuity of operations, and a comprehensive risk management strategy.

Information Assurance (IA): Joint Publication 3 -13 defines IA as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."

Confidentiality seeks to keep secrets secret. Integrity protects information from modification or compromise. Availability ensures that information and systems remain available in a contested cyber environment. Authentication provides a mathematical mechanism for one entity to establish its identity to another entity. Non-repudiation provides attribution of transactions in cyberspace, a potential enabler to both deterrence and friendly-fire avoidance in cyberspace.

Trust: Trusting a system requires trusting its hardware, software, and information. It is necessary to maintain trust in the information that these systems handle, both the integrity of data at rest and data in motion as systems evolve in capability and technology.

Threat Avoidance

Avoiding a threat provides a strategic defensive strategy that can reduce or eliminate the need to fight that threat. We propose a three-pronged approach to cyber threat avoidance. First, we employ deterrence to prevent the initiation of attacks. Second, we seek to make most threats irrelevant by modifying the cyber domain to eliminate vulnerabilities or make them inaccessible. Third, we use real-time agility through anticipation and escape maneuvers to evade the threat.

Deterrence: 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. Deception to influence adversary perception of costs, benefits, and the potential for retaliation also play a role in deterrence.

Effective employment of deterrence presumes a rational adversary to whom the perceptions of cost, benefit, and retaliation can be communicated. Deterrence also requires that the defender possess both the means and the will to retaliate to an attack.

Domain Modification: Modifying the cyberspace domain to eliminate vulnerabilities or make them inaccessible to an adversary provides a viable approach to threat avoidance. Sound hardware and software development practices can eliminate beforehand vulnerabilities by designing them out of a system. Since cyberspace qualifies as a man-made technological domain, we can rewrite the laws that define the domain and modify its behavior to favor protection and defense. The extension, modification, and replacement of protocols, architectures, hardware, and software are imperative to secure critical warfighting systems.

Polymorphic techniques offer a dynamic approach for continual and rapid multidimensional modification of the cyber domain. These modifications can take place many times per second if necessary, by varying protocols at multiple layers to deny an attacker SA and remove the advantages of time and preparation.

Agility: Agility in defense includes establishing indications and warning mechanisms that detect anomalous activities or entities, rapid analysis of the activity to include attribution and geolocation, anticipation of future behaviors and effects, and effective real-time provisioning of defensive measures.

Real-time threat avoidance presents an adversary with an agile moving target through evasion tactics, stealth, detection prevention, and non-identification. Self-aware defenses detect the failure of evasion tactics and confront an emerging threat with active escape tactics. In such instances, SA enables defensive agility via an accurate environmental context.

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 is enabled through predominantly defensive measures when tension pushes a situation away from peace towards conflict. In turn, these predominantly defensive measures enable the capabilities that support global power in the event of conflict escalation into major combat operations.

Access

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 space is essentially constant—the cyberspace domain changes dynamically, and increases indefinitely in size, creating unique technical challenges for the positioning of cyber assets.

Survival

An effective defense-in-depth avoids a large percentage 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, mission assurance seeks to ensure that critical MEFs fight through, and recover from, attacks against the underlying cyber infrastructure.

Survivability represents the quantified ability of a system, subsystem, equipment, process, or procedure to function continually during and after a disturbance. USAF systems carry varying survivability requirements depending on MEF criticality and protection conditions.

Fight Through: Existing approaches to information system security and survivability focus on preventing, detecting, and containing unintentional errors and intentional cyber attacks. The difficulty in automating the determination on whether a disturbance resulted from an error or an attack complicates autonomous recovery.

The concept of collaborative trusted agents that execute faithfully the commander's intent in the face of a dynamic cyber threat improves the potential for surviving and fighting through attacks. Through formal design methods and a self-protection guarantee, a class of general purpose agents can deploy special-purpose payloads to enhance the ability of a system to detect and fight through an attack, and can serve as a central launching point for system recovery.

Recovery describes the ability of a computer system to regain or even exceed its initial operating capability. While continuing MEFs, damaged systems must recover any lost services, components or data. These systems must discover their own vulnerabilities, identify the root cause of errors and attacks, and regenerate themselves with immunity to improve their ability to deliver critical services. Synthetic diversity ensures overall population survivability by removing like vulnerabilities of an otherwise vulnerable monoculture.

Since attacks in cyberspace happen in milliseconds, recovery must be automatic—not requiring human intervention. Automatic recovery requires a rapid understanding of the root cause of a failure or successful cyber attack. This knowledge must translate into the development and delivery of diverse, immune, and functionally equivalent code and components into a vulnerable system to restore it to a trusted state. Automatic recovery reconstitutes the system to its initial operating capability and decreases its vulnerability to similar attacks.

Mission-Aware Systems: The current DoD IA posture relies on solutions that seek to protect information and information systems, rather than the missions that depend on them. USAF systems must control dynamically end-to-end resources to provide mission aware service delivery and IA-enabled MA. These systems must adapt to failures and attacks by reconfiguring resources to provide an acceptable level of service and security. We must design and build systems that fight their way through attacks towards recovery, preserving MEFs while restoring system functionality and trust.

Cross Domain Operations

In Internet terminology, a domain refers to a group of computers or Internet protocol addresses that share higher-order addressing bits or higher-order naming convention. Consequently, computer security terminology calls cross-domain operations those transactions that occur across different classification levels, or across Internet domains at the same classification. In this document, we maintain consistency with the joint definition of domains as they pertain to warfighting domains, and we use the term cross-domain to represent operations across land, sea, air, space, and cyberspace.

The mission of the USAF "to fly, fight, and win ... in air, space, and cyberspace" requires an ability to maneuver through cyberspace as a means to attacking and defending from any domain against another. Effective cross domain operations require realistic modeling, simulation, and war gaming of the integrated effects among multiple domains, integrated planning of effects delivery, and cross-domain command and control.

Modeling, Simulation, and War Gaming: Robust modeling and simulation, and realistic war gaming, permit experimental pre-deployment, prototyping, and evaluation of cross-domain effects. The wartime employment of cross-domain capabilities guarantees robust and agile execution of the commander's intent, while ensuring cyber protection and MA across the command, control, communications, computers, intelligence, surveillance, and reconnaissance enterprise. Air Force warfighting systems rely on cyberspace operations, and these do not occur separately from air and space operations, but as an integrated interdependent operation.

Integrated effects modeling, simulation, and war-gaming must include the integrated delivery of effects from blue and red systems in every domain against red and blue systems in every domain. Integrated effects exercises must provide a realistic environment for cross-domain operations, in which activities in one domain have a direct bearing on activities in another domain.

Integrated Planning: Many parallels exist between operations in the more traditional domains of air and space and in the emerging domain of cyberspace. As we integrate these capabilities, planning requirements for cyber assets mirror those for tra-

ditional intelligence, surveillance and reconnaissance (ISR) and combat assets. The practice of procedural versus positive control over air assets and the time scales of the Air Operations Center do not translate well to cyberspace where decision cycles hover around a fraction of a second. Conversely, placing cyber assets under procedural control requires the incorporation into the operational tempo a set of previously agreed upon rules for a broad range of future scenarios.[3]

Integrated planning must take into consideration the challenges of cyberspace de-confliction, identification of friend or foe (IFF) procedures and the potential of cyber fratricide and cross-domain fratricide. The ability to tag and identify cyber assets and to ascertain continuously their status and integrity create technical challenges unique to cyberspace. In addition, the routine use of the global cyberspace commons necessitates extending IFF technology to individual sessions, transactions and packets.

Cross-Domain Command and Control: Cross-domain superiority enables MEF execution in a contested cyber domain and permits achieving and maintaining freedom of use of air, space, and cyberspace. Cross-domain dominance refers to the freedom to attack and the freedom from attack in and through air, space, and cyberspace. It permits rapid and simultaneous, lethal and nonlethal effects in these three domains to attain strategic, operational, and tactical objectives in all warfighting domains—land, sea, air, space, and cyberspace.[4]

The popular definition of cross-domain dominance suggests a choice among domains to deliver a desired effect against a traditional target. Under this definition, a cyber attack or a kinetic attack can deliver comparable effects against an intelligent target. Similarly, cyber countermeasures can play a cross-domain role in defending intelligent systems against a range of conventional and non-conventional threats.

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 warfighting 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 munitions, estimating first-, second-, and higher-order effects, and taking response action to external events.

Delivering Precision Effects

Precision effects are the intended outcomes of offensive operations in any warfighting 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.

Robust Effects: Cyberspace operations can produce strategic, operational, and tactical effects across the entire spectrum of conflict—from peacetime to major combat operations.

Sustained Cyberspace Operations: Second- and higher-order effects of cyberspace operations may extend beyond the immediate effects on a specific system. The complexity of estimating the duration and extent of cyber effects raises technical challenges unique to this domain.

Delivering Cross-Domain Effects: Cyberspace operations can create effects in other domains. The various effects upon adversaries and their systems are often categorized using the D-family of terminology: deter, deny, disrupt, deceive, dissuade, degrade, destroy, and defeat. Cross-domain effects delivery extends beyond the traditional warfighting domains of land, sea, air, space, and cyberspace, and includes the use of cyberspace as an auxiliary to national power to deliver diplomatic, information, military, and economic effects.

Cyber Effects-Based Assessment

Cyber effects-based assessment (EBA) refers to the process that provides the warfighter 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 that result from the application of cyber power.

Cyber EBA seeks to inform the commander of the mission impact of cyber operations. To this effect, cyber EBA requires a relationship between physical EBA (a router is down) and mission EBA (personnel system disruption). Mission planning geared toward EBA permits adequate pre-positioning of cyber sensors and assets and proper sequencing of operations and events. A distributed cyber sensor network provides a comprehensive multi-dimensional impact assessment capable of identifying and assessing changes to network status, system performance, and adversary behavior.

Effects on Systems: The first-level requirement for cyber EBA is to determine the effects of a cyber operation on a target system. Computers, network infrastructure, intelligent weapon systems, and critical infrastructure provide potential targets, and require specialized methods for assessing effects. Measures of effectiveness (MOE) and associated methods for measuring MOE are necessary to assess accurately the higher-order effects of a cyber operation against a target.

Effects on Users: A second application of cyber EBA includes determining effects on users. Specifically, if the intent of a cyber operation is to influence the thinking and actions of users, ranging in scope from a single user to a society of users, it is essential to develop the capability to assess the impact of cyber activity on behavior. A knowledge-based representation of human, organizational, cultural, and societal structures and behavior aids in this assessment.

Cyber Effects Assessment of Kinetic Operations: A third category of cyber EBA refers to assessing through cyber means the kinetic effects of traditional combat operations. This category includes capabilities for determining changes to network traffic and topologies before and after kinetic attacks to determine primary and secondary effects of kinetic attacks. This category includes also the seamless fusion of cyber ISR with traditional ISR collections.

Response Action

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.

Although RA focuses primarily on blue response to an asymmetric hostile cyber action that seeks to negate US superiority in a traditional domain, RA must become an integral part of operation planning in coordination with, and in response to, kinetic actions. Together, these active response actions seek to assure mission success in the last mile of force projection in the cyber domain.

Response Action for Attack Containment: Rapid forensics play an integral role in CND-RA by detecting attacks, attributing them to a source, estimating damage and enabling response COA to contain the attack and limit the damage. Additionally, rapid collateral effects estimate and battle damage assessment of contemplated RA permits automating such a response within the ROEs.

Offensive Response Action: A traditional view of cyber operations separates defensive activities from offensive activities. As attacks grow in sophistication and rapid response action requires automating ROEs, technical and legal challenges arise in using offensive operations to defeat an attack.

CONCLUSIONS

This article presented a S&T perspective on cyber operations within the focus necessary to operate in a contested cyber domain and to assure critical military missions in land, sea, air, and space against threats in cyberspace.

We recognize that the USAF depends vitally on cyberspace to achieve its vision of global vigilance, global reach, and global power. Further, the USAF projects global vigilance, global reach, and global power differently at various stages of tension across the spectrum of conflict. Consequently, the dependence of the USAF on cyberspace operations varies with the stage of conflict.

Global vigilance at peacetime requires persistent SA in all domains, mission and information assurance, and threat avoidance through deterrence and technology. Global reach requires access to the battle space, survival, and fighting through cyberspace attacks, and integrated planning of MEFs and their dependence on cyberspace.

Global Power calls for predominantly offensive combat operations, enabled through the delivery of precision effects in cyberspace, reliable effects assessment, and automated response action.

Notes:

[1] General Norton A. Schwartz, "Fly, Fight, and Win," *CSAF's Vector*, September 2008 .

[2] Definition of Situation Awareness as cited in M. R. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 (1995): 32-64.

[3] Procedural control - a method of airspace control that relies on a combination of previously agreed and promulgated orders and procedures, Joint Publication (JP) 3-01; 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.

[4] The Air Force 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, JP 3-30: "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, notes pages, Lt Col Brad "Detroit" Lyons, Lt Col Tim "Dexter" Rapp, Air Force Strategic Studies Group CHECKMATE, 10 June 2008.

Acknowledgement: This article summarizes the Strategic Vision for Cyber Operations Science and Technology developed by the Cyber Operations Innovation Team at the Air Force Research Laboratory Information Directorate in Rome, New York. The innovation team includes Scott Adams, Mark Gorniak, Todd Humiston, Patrick Hurley, Herb Klumpe, Paul Ratazzi, Paul Repak, Brian Sessler, James Sidoran, Jason Siegfried, George Tadda, Walt Tirenin and Thomas Vestal.

Dr. Kamal Jabbour, ST (BE Electrical Engineering with Distinction, American University of Beirut; PhD Electrical Engineering, University of Salford, UK) a member of the scientific and professional cadre of senior executives, is senior scientist for Information Assurance, Information Directorate, Air Force Research Laboratory (AFRL), Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. 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 other Air Force organizations, Department of Defense, and government agencies, universities, and industry.

Dr. Jabbour began his professional career on the computer engineering faculty at Syracuse University, where he taught and conducted research for two decades, including a three-year term as department chairman. In 1999, he joined the Cyber Operations Branch at AFRL through the Intergovernmental Personnel Act, and transitioned gradually from academia to government.

In response to President Bush's National Strategy to Secure Cyberspace, Dr. Jabbour created the Advanced Course in Engineering (ACE) Cyber Security Boot Camp to develop the best ROTC cadets into future cyber security leaders. The ACE combines advanced academic training, hands-on internships, officer development, and weekly eight-mile runs into a challenging cyber security boot camp. The ACE received designation of a Special Interest Item for its role in developing officers for the new Air Force Cyberspace Command.

Dr. Jabbour has received one US patent, published more than 60 papers in refereed journals and conference proceedings, and supervised 21 theses and dissertations. An avid distance runner, Dr. Jabbour wrote a weekly column on running in the *Syracuse Post-Standard* from 1997 to 2003.