

AIR, SPACE, AND CYBERSPACE POWER IN THE 21ST CENTURY

38th IFPA-Fletcher Conference on National Security Strategy and Policy

January 20 – 21, 2010

DAY ONE

SESSION 4

5:00 TO 6:30 P.M.

The Science and Technology of Cyber Operations

Dr. Kamal Jabbour, ST

Air Force Senior Scientist for Information Assurance

20 January 2010

The US Air Force vision of global vigilance, global reach and global power drives the science and technology requirements for cyber operations. My remarks this afternoon will focus on the front end of the acquisition chain, as I explore the challenges of developing cyber technologies to enable US military superiority in land, sea, air and space, and to provide another domain where the US can deliver effects.

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.

We identify (1) situational awareness, (2) assurance, and (3) threat avoidance as the three main capabilities necessary to achieve global vigilance in and through cyberspace.

The strategic objective of cyber **Situational Awareness** is to provide automated situation assessment and analysis that meet the operational requirements of all missions within the cyber domain—friendly blue missions, adversary red missions and traversal gray systems in the global commons. Mission awareness, the ultimate objective of situational awareness, requires understanding the dependence of missions on specific cyber assets, the interdependence of assets and the interdependence of missions.

Mission Assurance Is a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. The reliance of mission essential functions on cyberspace makes cyberspace the target of choice for an adversary who cannot, or chooses not to, face us in conventional battle. To assure mission-essential functions in a contested cyber

domain requires mapping mission dependence on cyberspace, prioritizing missions and managing risk to ensure continuity of operations.

Strategic Threat Avoidance can reduce or eliminate the need to fight threats. Threat avoidance starts with deterrence to prevent the initiation of attacks. Second, cyber domain modification can render many threats irrelevant by eliminating mission vulnerabilities or making them inaccessible. Third, real-time agility through anticipation and escape maneuvers can evade persistent threats.

Effective Deterrence in Cyberspace requires manipulating the cost-benefit ratio into a disincentive by increasing the cost of an attack and lowering its perceived benefits. Deception to influence adversary perception of costs and benefits may play a role in deterrence, and presumes a rational adversary to whom these perceptions can be communicated.

Cyber Domain Modification to eliminate vulnerabilities or make them inaccessible to an adversary provides a viable approach to threat avoidance. Sound hardware and software development can eliminate vulnerabilities by designing them out of a system. The extension, modification and replacement of protocols, architectures, hardware and software are necessary to secure critical war-fighting systems. Polymorphic multidimensional modification of the cyber domain, many times per second if necessary, by varying protocols at multiple layers can deny an attacker the benefits of time and preparation.

Agility presents the adversary a moving target through evasion and stealth. Self-aware systems detect a failure of evasion tactics and confront an emerging threat with active escape tactics.

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.

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, creating unique technical challenges for positioning cyber assets.

An effective defense-in-depth avoids a large percentage of attacks. However, when an attack disrupts US systems, the defensive priority turns to **survival** and mission assurance that ensure continual operation during and after a cyber attack.

Fight Through: 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. Formal design methods and a self-protection guarantee can enhance the ability of a system to fight through an attack, and can aid in system recovery. Synthetic diversity ensures overall population survivability by removing like vulnerabilities of an otherwise vulnerable monoculture.

Mission-Aware Systems: An IA posture that seeks to protect information and information systems may fail to assure the missions that depend on them. Mission-aware systems must control dynamically end-to-end resources to provide mission-aware service delivery and IA-enabled MA. These systems must adapt to attacks by reconfiguring resources to provide an acceptable level of service and security.

Cross Domain Operations refer to attack and defense from any war-fighting domain - land, sea, air, space, and cyberspace - 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.

Robust Modeling and Simulation, and Realistic War Gaming permit experimental pre-deployment prototyping and evaluation of cross-domain effects. Integrated effects modeling, simulation, and war-gaming must include the integrated delivery of effects in every domain against red and blue systems.

Integrated Planning must take into consideration the challenges of cyberspace de-confliction, identify-friend-or-foe procedures and cross-domain fratricide. The ability to tag and identify cyber assets and to ascertain continuously their status and integrity creates unique technical challenges.

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. The global projection of cyber power to complement or enable kinetic power creates technical challenges of developing precise cyber munitions, estimating first-, second-, and higher-order effects.

Delivering Precision Effects is the intended outcome of offensive operations in any war-fighting domain. For 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 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 strategic, operational, and tactical effects across the entire spectrum of conflict—from peacetime to major combat operations. Second-order and higher-order effects of cyberspace operations may extend beyond the target system to become an auxiliary to national power by delivering diplomatic, information, military and economic effects.. The complexity of estimating the **robustness, duration and extent** of cyber effects raises technical challenges unique to this domain.

Cyber Effects-Based Assessment seeks to quantify the outcome of a cyber operation in near real-time during the prosecution of a mission by fusing multiple sensors and combining multiple means of measuring effects. Developing measures of effectiveness (MOE) and associated methods for measuring MOE is necessary to assess accurately the higher-order effects of a cyber operation against a target.

If the intent of a cyber operation is to influence the thinking and actions of a user or a society of users, it is essential to develop a knowledge-based representation of human, organizational, cultural, and societal structures and behavior.

IN CONCLUSION - we presented a Science and Technology 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 from cyberspace.

We recognize that the USAF depends vitally on cyberspace to achieve its vision of global vigilance, global reach, and global power.

Global vigilance requires persistent situational awareness 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 mission essential functions and their dependence on cyberspace.

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