Document created: 4 April 00
Air & Space Power Chronicles - Chronicles Online Journal

Cyber Attack Response:
The Military in a Support Role

by

Col(S) Nonie C. Cabana

"*The enemies of peace realize they cannot defeat us with traditional means. So they are working on new forms of assault: cyber attacks on our computer systems*"[1]

President Clinton

Introduction

This article will examine the military support role regarding cyber attack to the U.S., the consequences and implications, and offer possible alternatives to strengthen our homeland defense against cyber attack. It contends that the DOD should not lead the counter cyber attack efforts based on three likely scenarios: 1) transportation infrastructure; 2) financial institutions; and 3) public services.

There is general agreement today that technology is changing the way future warfare would be conducted--especially on the use and vulnerabilities of computer information systems.

Before World War II, the Atlantic and Pacific Oceans served as defense firewalls to protect the United States from enemy attack. The Japanese attack on Pearl Harbor in 1941, however, suddenly challenged our invincibility and made us question our ability to withstand further attack. Unfortunately, winning the war on both fronts caused our fears to fade. John Gilligan, Director of Information Technology/Systems, Department of Energy, summed it up well when he stated: "The state of the art is such that, while we are putting up protective barriers and firewalls and such, there is a general agreement that there are no 100% guarantees."[2] Richard Clarke, the National Coordinator for Security, Infrastructure Protection and Counterterrorism further stated: "an attack on Americans cyberspace is an attack on the United States that should trigger a military response."[3]

Assuming a foe launched a cyber attack on the U.S., what role should the military take in response? Should the military take the lead because others view cyber attack as both an act of warfare and a

national defense issue? Both cyber and biological agent attacks cross this difficult line. What makes these attacks different from a nuclear warhead delivered by a missile? The distinction seems to hinge on whether the issue is 1) to defend against a cyber attack, or 2) to deal with the domestic consequences of the attack.

If the military takes the lead role in the cyber attack defense, it should be prepared to deal with possible resistance from other federal agencies such as the Federal Emergency Management Agency (FEMA) or the Department of Justice. Some say the Departments of Commerce, Treasury, Health and Human Services, Energy, Transportation, State, and the Environmental Protection Agency, could also play key roles, depending on the cyber attack target. The military should embrace the supporting role during a cyber attack to the homeland until the cyber attack is clearly defined as a threat to our vital interest and the responsibility among federal agencies is delineated.

Moreover, a litmus test is needed to assess whether the cyber attack even constitutes a direct attack to our vital interests national security, homeland defense, and economic prosperity. When does a cyber attack become a weapon of mass destruction or mass disruption? Shall a distinction be made between destruction and disruption to craft an appropriate military response? No doubt, this issue requires further discussion and exploration to produce a realistic and workable strategy.

Another challenge is finding the perpetrator because it could simply be curious children/teenagers or disgruntled citizens. On the other hand, if hostile nations or known terrorists initiated the attack, the U.S. military should likely retaliate.

Conversely, the military lead role outside the homeland is well defined. For instance, the military played an active cyber war role in Kosovo. Bob Brewin, *Federal Computer Week*, reported that a London-based spokesman for U.S. Naval Forces, Europe, confirmed that "it was the first time a Joint Task Force staff was organized with an information operations (IO) cell, which was composed of military personnel with expertise in various facets of IO.[4] The IO cell objective was to disrupt Serbias' computer systems to give the U.S. and her allies the winning edge in the information warfare.

Background

The age of cyber attack presents a new challenge to the military. A 1999 Reuters, Washington Post article for example stated: "organized attacks such as 'solar sunrise' on DOD computers in February 1998, and computer viruses such as 'Melissa' early this year, highlight the government's susceptibility."[5] Further, Executive Order 13010, July 15, 1996, "defines certain national infrastructures as so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[6]

Although we may eventually know the spot of origin of a cyber attack, finding its perpetrator may be an even greater challenge. Complicating this dilemma is "the threat is going to be death by a thousand cuts, rather than a giant attack."[7] Russian "cyberspooks" may have recently infiltrated U.S. computer security.

The operation coined "Moonlight Maze,"targeted information on classified naval codes and missile guidance systems.[8] The attack may have been committed by a person or persons not connected to the government, who were upset at the U.S. over the Kosovo affair;[9] however, no one knows for sure. Does this event then warrant a military retaliation? The answer should be a resounding "no", since there was no immediate threat to our interest and the chief instigator was unknown. For the U.S. to retaliate, there has to be a direct attack by a rogue nation or known terrorist to our critical information infrastructure such as electrical grids and transportation nodes, which falls under our economic and security interests.

As we wrestle with this new form of asymmetrical warfare, we need to produce a litmus test and assess the military's possible role before we face the inevitability. Failure to do so invites unnecessary risks that further increase military operational tempo.

Transportation Infrastructure:

Disabling the transportation computer systems operating our highways, railroads, waterports and airports could degrade our vital interest--economic prosperity and military readiness. For example, a cyber attack on Savannah Water Port's, Georgia, Bell South's switching systems "would make it impossible to deploy military forces at the pace specified in operations plans."[10] Protecting a commercial waterport like Savannah involves several government agencies including the Departments of Transportation, Commerce, Justice, Defense, and other agencies. A report prepared by a top-level Defense Department advisory panel summarized the DOD position: "We should not forget information warfare as a form of warfare, not a crime or act of terror." The report further made this point: "The response could entail civil or criminal prosecution, use of military force diplomatic initiatives or economic mandates."[11] Thus, the Departments of Defense, Justice, States, and Commerce all have legitimate roles to play in dealing with this war on information systems.

A 1999 *Defense News* article stated: "Tomorrow's threats will require a responsive apparatus to support U.S. decision-makers. Today's sprawling, tangled network of agencies and staffs simply cannot do the job."[12] Clearly, this issue deserves a closer look and increased attention from our Administration; for if we fail to address it, we may find that we have indeed "met the enemy," and he may be us. The ultimate losers would be the American people.

Our transportation vitality thrives because of its robust and cutting-edge computer systems. A massive attack on these systems could spell instability and chaos at the highest order. Computer reliance "has created a tunnel of vulnerability previously unrealized in the history of conflict and could have a catastrophic effect on the ability of DOD to fulfill its mission."[13]

Another way cyber attack can impair our defense posture would be through manipulation of data in the Global Transportation Network (GTN). The U.S. Armed Forces uses this system for "intransit visibility, command and control (C2) applications, and business decision support tools."[14] Assuming that hackers successfully broke into the GTN, what would happen when GTN data showed that critical combat troops and equipment were in place in the computer data, but in reality, were not. This predicament would not

only cause unnecessary requisition requests for additional resources but would also throw-off the warfighter's decision making process.

However, does this potential impact compel DOD to take the leading role? Although this situation affects national security, it would not reach a crescendo to warrant the military taking the lead. That is, experiencing temporary transportation setbacks may occur, but America's robust technology, coupled with her "societal agility," would find a way to overcome this problem. If on the other hand, gathered intelligence showed the nation states or known terrorists launched this specific attack to impair U.S. vital interest, then the military should exercise the option to respond.

A computer failure in the transportation infrastructure goes beyond its immediate platform. This was illustrated by Slabodkin's August 31, 1999 article, which depicted the U.S. Navy's Aegis cruiser *Yorktown*, a test bed for its Smart Ship Program, was "dead in the water" for several hours due to "a basic programming problem."[15] This incident represented what an adversary could do to our combat ships without firing a missile or conventional weapon. What action should the military take? Clearly, no conventional weapon was used. What level of retaliation would be appropriate, and when should it be directed? Since this scenario did not identify the enemy and did not impact the vital interest, the military should take a role in support of the federal lead agencies and not lead the effort itself. Such an attack would present a complex dilemma for the Interagency Working Group in the National Security Council determining exactly who should lead.

Clearly, there are many stakeholders in the decision making process whom have equally important roles in the process. Each agency could legitimately take the lead. A decision matrix might institute a process to optimize leadership responsibility.

Paralysis of Financial Institutions

The advent of computer capability to electronically transfer funds and make payments has enhanced the global economy and forever changed the way we do business. Hence, a cyber attack to this institution is an attack to our vital economic interest. Statistics indicate that over the last five years at least 25 percent of economic growth are attributed to information technologies.[16] John Hamre, Deputy Secretary of Defense, illustrated the impact of monetary transactions: "Every month we write about 10 million paychecks. We write about 800,000 travel vouchers. One of our finance centers disburses $45 million an hour."[17] The Tampa-based Armed Forces Financial Network (AFFN) employs "more than 30,000 ATMs in more than 30 countries and on two Navy ships," which equates to a total of "more than 60-million cardholders."[18] The military is also working with AFFN to develop a smart card "that can serve as a combination ID card, meal ticket and cashless charge card."[19] It would be a powerful attraction for terrorists to make a cyber attack on those electronic cardholders. Without firing a single shot, they could achieve the significant accomplishment of upsetting morale and creating economic chaos within the military-civilian establishment and financial community.

Equally important, panic and hysteria created by a successful cyber attack on financial institutions such

as the World Trade Center or the Wall Street could cause the public to lose confidence and trust in our government because it would have failed to protect the American interest. In the words of Martin van Creveld, *The Transformation of War*, "the most important single demand that any political community must meet is the demand for protection."[20] The military must be cognizant of the fact that federal agencies such as FEMA, DOJ, and others may be placed in charge of protection and possible reaction on issues clearly domestic in nature. These agencies are better adept in this field.

Our interagency coordination machine is lacking a tool to put all these agencies under a single command and control umbrella that would perform like a military theater unified Commander-in-Chief or joint task force. Although, this issue is being addressed, it has not yet produced a viable alternative to the present policy. In spite of damaging, degrading and paralyzing financial institution and risking the domino effect of this paralysis to our national economy and security, the military should apply restraint and prudence. It should not be tempted to take charge of matters clearly under the lead charter of other federal agencies. Rather, prudent judgment by civilian and military senior leaders must prevail in providing military assistance to the designated lead federal agency without creating the perception that the military "has taken over." Exception to this rule, nevertheless, applies when the nation states or known terrorist initiated the attack to destabilize our vital interest. At this juncture, the military response becomes reasonably appropriate.

On the other hand, when the situation calls for a leader, the military organization should respond. Recall the military's proactive stance to establish an Information Operations cell within the Joint Task Force in the war in Kosovo.[21] Granted, the military believed it had identified the perpetrators, and the American public distanced itself from this attack, for it did not directly affect the vital interest. On the homeland, however, determining the enemy is tougher. Here, the enemy may just be a curious child or student anxious to see how far he/she can go. Hence, reliance on lead federal agency is the best option to deal with this domestic issue.

Public Services

Continuous improvement of information technology makes our 911 emergency service support system an integral and reliable part of community service. Nevertheless, because the 911 service affects us all, it has become a potential cyber attack target. A Los Angeles Times article reported "the Red Team hackers hit the jackpot they broke into networks that direct the 911 emergency response systems."[22] Does this act, then, represent a direct attack to our vital interests? Arguably so. After all, this attack violates our individual safety and promotes fear among the populace, both of which are inseparable to our vital interest. Consequently, if the evidence shows the attack originates from rogue states or known terrorists, a military response should remain an option to punish the perpetrators.

Equally important, is the absence of telecommunications capabilities, which could severely disrupt fire department and ambulance services. Delay of legitimate emergency response could mean life or death to hundreds of victims. Like the 911 issue, this dilemma undoubtedly smacks our core values to protect and save lives. Hence, this situation can also be viewed as a direct attack to our vital interest, which warrants

an appropriate military action. Absent this evidence, the military should take the supporting role.

Several federal agencies could take the lead in response. Some say the Department of Justice could lead because criminal acts may have occurred. Others view FEMA fit the bill because government services have essentially stopped.

The Dilemma for the Military

The military is not trained to enforce civil laws. Further, the Posse Comitatus Act prohibits military employment for direct law enforcement.[23] An attempt to change this act should be avoided for the U.S. clearly has adequate law enforcement agencies to effectively deal with civil laws. In short, the military should shy away from law enforcement issues clearly internal and domestic in nature. To stay on track, federal, state, and local enforcement agencies must work hand in hand with the military to preclude violation of the Constitution when dealing with cyber attack cases in the U.S. For instance, the military should not "cross the line" when it supports the federal agencies to counter drug operations and control the flow of illegal immigrants crossing our borders. The same principle of restraint should apply to a cyber attack. There has to be an agile command and control instrument that puts the best lead agency to deal with situational cyber attacks.

Another dilemma facing the military is the containment of cyber attack. For no matter how much preparation is done to counter cyber attack, it can happen anytime and anywhere. Cyber attack circumvents boundaries. In the words of Admiral Bud Edney, USN (Ret.): "Borders are no defense for the penetration of information even in a highly controlled or authoritarian societies."[24] Countering this dilemma may require some investments on Research and Development to enhance the penetration detection system.

Consequences and Implications of Military Role

Twentieth century America is not accustomed to seeing its military involved in domestic affairs, except during national disasters, emergency, and riot situations. Nevertheless, examples of the military providing disaster relief to the community is not unprecedented. Recall military assistance in the "Oklahoma City bombing" during this decade.[25] Our Constitution clearly defines the role of the military to be subordinate to civilian authority. The Honorable John J. Hemre, Deputy Secretary of Defense, made it clear that "DOD’s mandate is to provide assistance to appropriate federal civilian authority--either the Department of Justice or the Federal Emergency Management Agency Hamre further states: "there are no plans to create a ‘Homelands Defense Command’ or any other military institution to oversee civilian-led response efforts."[26] He is right. The American people nurture this special relationship.

Moreover, the military’s allegiance to the President as Commander-in-Chief makes it the "force of choice" to deliver results without political squabbling. Nonetheless, traditions, ethics and the military ethos compel the military to be sensitive in taking the lead for fear of public rebuke impeding citizens’

civil rights. For example, Mr. Weiner's August 16, 1999 article in New York Times illustrated this fear when "Congress has blocked money for a planned system to safeguard government computers, a prominent Republican has denounced the system as "Orwellian," and some civil libertarians are calling this system a potential threat."[27] One way of avoiding this criticism while at the same time engaging the populace, however, is show the general public that the military would take appropriate action to punish the nation states or known terrorists responsible for attacking our homeland's vital interest based on intelligence and military resolve.

Regarding the year 2000 computer problem potential havoc to our way of life, DOD's position is to remain noncommittal. Some may argue that DOD should assist the citizens because of its oath to "support and defend the Constitution against all enemies foreign and domestic." However, DOD position on this issue is "year 2000 problem becomes an enemy only if nation states or terrorists use it as an opportunity to attack U.S. interest."[28] At what point then does an attack inflicting damages to our vital interest, but uses non-traditional mechanisms become a proper role for the military? How does this scenario differ from a missile attack to our homeland? One answer is that we are now working on a national missile defense technology to shoot it down in the mid-air before it lands on large populated areas. On the other hand, we have not developed a similar defense technology to thwart a cyber attack making it more difficult for us to identify the enemy or perpetrator.

Another challenge facing the military is the complexity of defining weather a cyber attack constitutes a weapon of mass destruction or a weapon of mass disruption. Knowing the difference between these two issues may help the military craft its appropriate response.

The recent designation of U.S. Atlantic Command to U.S. Joint Forces Command continues the tradition of providing military assistance to civil authorities in the event of a nuclear or biological attack within the U.S.[29] A cyber attack could also fall under this military assistance program.

Moreover, The Armed Forces Journal, October 1999 issue, captured a Marine Corps officer's sentiment participating in Exercise Urban Warrior in the CONUS when he said: "I would put down my arms and walk away if the armed forces were to do anything against the American people."[30] This unique distinction of respecting the civil rights of the American people is a powerful reminder to the military for not assuming lead roles in matters clearly under the auspices of other federal agencies. USA Today, recently reported "the military continues to enjoy the respect from the American public because it does not threaten the interest of any American and it has remained above politics."[31] The message is clear for the military to assume a supporting role in this arena.

Paraphrasing Mr. Sullivan's and Mr. Harper's statement, ultimately, the military support to the community is based on providing basic needs, ensuring public health, providing open communications, and assisting in the rapid return of civil society with its duly constituted government.[32] This is one facet the military can touch the hearts and minds of the American people, and, in turn, win their trust and confidence.

Facing the Future

The military's ability to organize and coherently respond to crises is a national asset. Therefore, its assistance to public and private sectors is crucial in protecting the well being of our nation. Other lead agencies would be well served to emulate the military's command and control structures to achieve unity of effort. Several recommendations are worthy of further exploration:

A. Consolidate interagency guidance. According to the GAO, "Federal Agencies have not completed interagency guidance and resolved command and control issues."[33] The Federal Response Plan is a good starting template. It is working well for FEMA and other agencies during consequence management. It should include annex(es) that deal with cyber attack.

B. Elevate the title of National Coordinator to Director for Security, Infrastructure Protection and Counter Terrorism. Put teeth into implementation of Presidential Decision Directive 63 on Critical Infrastructure Protection that covers cyber attack.[34] Elevating his title would put him in equal status with FEMA Director, Attorney General, and the "Drug Czar." This elevation, naturally, would not eliminate the challenges of working with peers and solidifying relationships with the private sector representing multiple interests. However, this elevated title would give him an equal footing among the lead federal agency directors to espouse his agenda. On the flip side, an extreme caution and sensitivity should prevail to avoid a negative perception of abuse of power affecting citizens' civil rights as a result of this title elevation. Recall J. Edgar Hoover's legacy as the FBI director.

C. Keep the private sector engaged. A dialogue has been initiated via the Information and Sharing Analysis Center (ISAC) to keep the industry engaged. Moreover, under the Presidential Decision Directive 63, ISAC was allowed to "gather, analyze, sanitize and disseminate private information from the National Information Protection Center for further distribution to the private sector."[35] The idea was designed so "the ISAC may emulate particular aspects of such institutions such as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors."[36]

Despite this dialogue, the private sector is still driven by profit. There must be a "carrot" to get the private sector engaged. Otherwise, their full cooperation in cementing a responsive public-private partnership remains hallow. J. Douglas Beason, author of "DOD Science and Technology," was correct when he said: "Industry will not step up to fill a void unless there is a sufficient profit."[37] Possible incentives for the private sector might be tax breaks or other governmental relief.

D. Integrate cyber attack impact to U.S. Joint Forces Command's Joint Task Force for Civil Support's training program to address strengths and weaknesses of state and local computer defense mechanisms. This initiative may require extra efforts since the task force appears to be more focused on dealing with disasters caused by the Weapons of Mass Destruction (WMD).

E. Integrate the lead agency (Sector Liaison Official) with the private sector (Sector Coordinator)

to assess and develop a workable course of action.[38] State and local government agencies should maximize benefits offered by the public and private sector at the national level. Fostering a dialogue is essential for the existence of public service support to the community. Ultimately, the objective is to make the public and private sectors more aware of the military support role in their community.

In sum, the military role should be supporting, not supported for cyber attack defense. Exception to this rule applies if the attack is initiated by rogue nations or known terrorists against our vital interest or conditions where the military is best suited for the mission. For domestic consequence of a cyber attack, the military role should also be supporting.

In conclusion, the military can perpetually maintain the highest respect and admiration from the American people by defending the homeland against a cyber attack from rogue nation states and known terrorists. Taking the supporting position on the defense of cyber attack and domestic consequence platform would allow the military to distance itself from getting entangled with civil matters affecting domestic law enforcement. At the same time, the military should simultaneously assist agencies to better prepare them against cyber attack and improve their homeland cyber attack defense. This arrangement is a win-win situation for our nation.

Notes

1. The White House Office of the Press Secretary, "Remarks by the President On Keeping America Secure For the 21st Century," January 22, 1999, www.whitehouse.gove/WH/new/htm1/19990122-7214.html, August 31, 1999.
2. Bob Drogin, "In Theory, Reality, U.S. Open to Cyber-Attack," *Los Angeles Times,* October 9, 1999, p.16.
3. Tim Weiner, "Author of Computer Surveillance Plan Tries to Ease Fears," *New York Times,* August 16, 1999, p.1.
4. Bob Brewin, "Kosovo Ushered in Cyber War," *Federal Computer Week,* September 27, 1999, p.1.
5. Reuters, "GAO Cites Computer Security Risks," *Washington Post,* October 4, 1999, p.7.
6. The White House, Office of the Press Secretary, *Executive Order 13010,* July 15, 1996.
7. John Markoff, "Cyberwarfare Breaks the Rules of Military Engagement," *New York Times,* October 17, 1999, p.1.
8. Gregory Vistica, "We’re in the Middle of a Cyberwar," *Newsweek,* September 20, 1999, p.52.
9. Daniel Verton, "Russia Hacking Stories Refuted," *Federal Computer Week,* September 27, 1999.
10. Bob Brewin and Heather Harreld, "U.S. Sitting Duck, DOD Panel Predicts," *Information Warfare,* November 11, 1996, www.fcw.com/pubs/fcw111/duck.htm, August 31, 1999.
11. Ibid.
12. "Panel Lacks Inspiration," *Defense News,* October 4, 1999, p. 26.
13. Bob Brewin and Heather Harreld, "U.S. Sitting Duck, DOD Panel Predicts," Information Warfare, November 11, 1996, www.fcw.com/pubs/fcw111/duck.htm, August 31, 1999.
14. Global Transportation Network: "A USCINCTRANS Update," *Defense Transportation Journal,* August 1999, p.8.
15. Gregory Slabodkin, GCN staff, "Navy CIO Orders an Investigation of Yorktown Systems

Failure," www.cs.virginia edu/~survive/NEWS/news003.txt, August 31, 1999.
16. The White House, Office of the Press Secretary, Press Briefing by Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and Jeffrey Hunker, Director of the Critical Infrastructure Assurance Office, May 22, 1998.
17. The White House Office of the Press Secretary, Press Briefing, September 16, 1998, Appendix F.
18. Jeff Harrington, "Arming the Armed Forces With Access ton Cash," *St. Petersburg Times,* September 19, 1999, p. 1H.
19. Ibid.
20. Martin van Creveld, *The Transformation of War,* The Free Press, 1991, pp.197-198.
21. Bob Brewin, "Kosovo Ushered in Cyber War," *Federal Computer Week,* September 27, 1999, p.1.
22. Bob Drogin, "In Theory, Reality, U.S. Open to Cyber-Attack," *Los Angeles Times,* October 9, 1999, p. 16.
23. Military Assistance for Civil Disturbances, Federal Laws, Posse Comitatus Act, Section 1385 of Title 18, U.S. Code.
24. Admiral Bud Edney, USN (Ret.), "Thought on Rapid Dominance," *Shock & Awe,* National Defense University Institute for National Strategic Studies, November 1999, p. 145.
25. Federal Emergency Management Agency, Oklahoma City Bombing, Briefing Book, 1-3 (1995).
26. John J. Hamre, Deputy Secretary of Defense, U.S. Military wants no Domestic Law-Enforcement Role, *USA Today,* October 5, 1999, p. 16.
27. Tim Weiner, "Author of Computer Surveillance Plan Tries to Ease Fears," *New York Times,* August 16, 1999, p.1. http://ebird.dtic.mil/Aug1999/s19990817author.htm, August 26, 1999.
28. "DOD Is Right to Sit Out Y2K," *Federal Computer Week,* August 30, 1999, p.1.
29. Jack Dorsey, "Cohen Warns of Perilous Global Times," *The Virginia Pilot,* October 8, 1999, p. B4
30. Jason Sherman, "Invading Virginia," *Armed Forces Journal,* October 1999, p.16.
31. Terrorist Attack in U.S? Don't Put Military In Charge," *USA Today,* September 30, 1999, p.19.
32. Gordon R. Sullivan and Michael V. Harper, *Seeing the Elephant, Hope Is Not A Method,* Times Books, Chap 5, p. 85
33. *Reuters,* "GAO Cites Computer Security Risks," Washington Post, October 4, 1999, p.7.
34. White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 1998, Section IV, A Public-Private Partnership to Reduced Vulnerability, www.gsa.gove/ciao/, August 31, 1999.
35. Ibid., Appendix F-12.
36. Ibid., Appendix F-12.
37. J. Douglas Beason, "There Ain't No Such Thing As A Free Lunch," DOD Science and Technology, p. 98.
38. White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 1998, Section IV, A Public-Private Partnership to Reduced Vulnerability, www.gsa.gove/ciao/, August 31, 1999.

Disclaimer

The conclusions and opinions expressed in this document are those of the author cultivated in the freedom of expression, academic environment of Air University. They do not reflect the official position of the U.S. Government, Department of Defense, the United States Air Force or the Air University.

This article has undergone security and policy content review and has been approved for public release IAW AFI 35-101.

[*Air & Space Power Chronicles* Home Page | Feedback? Email the Editor]