Asymmetrical Threats:

A Vital Relevancy for Information Operations

LTG Kevin T. Campbell
Commanding General,
U.S. Army Space and Missile
Defense Command/U.S. Army
Forces Strategic Command

America's unrivaled military superiority means that potential enemies — whether nations or terrorist groups — that choose to attack us will be more likely to resort to terror instead of conventional military assault. Moreover, easier access to sophisticated technology means that the destructive power available to terrorists is greater than ever. Adversaries may thus be tempted to use unconventional tools, such as weapons of mass destruction, to target our cities and disrupt the operations of our government. They may try to attack our economy and critical infrastructure using advanced computer technology. [1]

The above citation, taken from Presidential Decision Directive 62 signed in May 1998, foresaw the potential that unconventional methods of warfare could be used against our Homeland. Although much has changed since publication of this document to address vulnerabilities, the threat remains for adversaries to attack our Nation, interests and military forces by unconventional or asymmetric approaches.

The end of the Cold War resulted in significant realignments of alliances and an increase in regional instabilities. The former Soviet Union, once the predominant threat to American security, has been supplanted by rogue and failed states and non-state networks and actors. These entities attempt to avoid confrontation with our conventional military capabilities by striking weak points in our Nation's social, economic and political structures, or by taking advantage of perceived U.S. military vulnerabilities. They often attempt to operate at the extremes of the conflict spectrum. At one end, North Korea is actively pursuing nuclear weapons capabilities. At the other end, groups such as al-Qaeda, remnants of Saddam Hussein's former Ba'athist regime and various sectarian militia groups pursue insurgency warfare using asymmetrical approaches.

Adversaries increasingly respond to U.S. military dominance by pursuing indirect, unorthodox or surprising approaches, and using the capabilities of information technology, especially the Internet, as a tool of asymmetric warfare. Because of this, Information Operations has emerged as a critical component of the Army's operational readiness. Information Operations is defined as, "the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own." [2] Space professionals, by their access to and understanding of the relationships between the core Information Operations capabilities, are particularly well qualified to support Information Operations against asymmetric threats.

Asymmetric Warfare: An Ongoing Challenge in Our Current Security Environment

Asymmetric warfare deals with one force attempting to circumvent or undermine strengths while exploiting weaknesses by using methods, nontraditional tactics, weapons or technologies that differ significantly from expected methods of operation. In essence, asymmetrical warfare is acting, organizing and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative or gain greater freedom of action. [3] Asymmetric warfare approaches can be applied across the spectrum of military operations.

Asymmetric warfare is a relative concept. The means of warfare by one group might be considered "asymmetric," while for the other group the means would merely be viewed as using all means available. As an example, "to the

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**
4. TITLE AND SUBTITLE **Asymmetrical Threats: A Vital Relevancy for Information Operations**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Space & Missile Defense Command,Army Forces Strategic Command,Redstone Arsenal,AL,35809**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR’S ACRONYM(S)
		11. SPONSOR/MONITOR’S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **Same as Report (SAR)**	18. NUMBER OF PAGES **6**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

> **Asymmetric warfare is a relative concept. The means of warfare by one group might be considered "asymmetric," while for the other group the means would merely be viewed as using all means available … "to the al-Qaeda fighter cowering in a cave in a remote part of Afghanistan, fuel air explosives dropped with deadly precision from aircraft miles away and thousands of feet up, directed by laser designators wielded by highly trained and stealthy special operations forces, is as asymmetric to him as his tactics are to us.**

al-Qaeda fighter cowering in a cave in a remote part of Afghanistan, fuel air explosives, dropped with deadly precision from aircraft miles away and thousands of feet up, directed by laser designators wielded by highly trained and stealthy special operations forces, is as asymmetric to him as his tactics are to us." [4]

Although a variety of descriptions can be found, the characteristics of approaches that generally are deemed to be "asymmetric" from an American military standpoint include: [5]

- "unusual" threats, e.g., taking and torturing hostages;
- "irregular" threats unrecognized by the practice and laws of wars, treaties and arms control agreements, e.g., nuclear explosions to disrupt satellite operations;
- "unmatched" threats that look different from war, e.g., the attacks of Sept. 11, 2001;
- threats highly leveraged against U.S. military and civil assets, e.g., ballistic missiles and weapons of mass destruction;
- threats that are difficult to respond to in kind, e.g., terrorism and weapons of mass destruction;
- threats difficult to respond to in a discriminate and proportionate manner, e.g., nuclear terrorism, guerrilla warfare and sabotage;
- "unknown" threats, e.g., ramifications resulting from an extensive attack with biological weapons.

Old and New Capabilities as Evolving Threats

Our Nation's adversaries currently attempt to employ a variety of weapons and capabilities in both conventional and unconventional ways to achieve their desired effects. A frequently cited example of an asymmetric approach is the use of Improvised Explosive Devices (IEDs), the leading cause of casualties for our warfighters in Iraq. In the majority of cases, one or more artillery projectiles are command detonated using a variety of triggering devices. In August 2006 alone, approximately 1,200 IEDs were detonated as insurgent forces continue to invent new ways to design and hide these lethal munitions. [6]

By relying on IEDs as a means of attack, insurgent forces attempt to create a situation where our combat forces have difficulty in identifying adversaries to engage. [7] In several instances, videos showing insurgent attacks using IEDs have been uploaded to popular Internet video-sharing sites, such as YouTube and Google Video. [8] The result is that insurgents have now seized the initiative in conveying their messages to a worldwide audience in a manner that is not subject to widely accepted journalistic standards.

The greatest concern of asymmetric approaches is the use, or threat of use, of weapons of mass destruction by terrorists, including their employment with missiles. As stated in the most recent Quadrennial Defense Review Report, "Our enemies seek weapons of mass destruction and, if they are successful, will likely attempt to use them in their conflict with free people everywhere." [9] GEN James Cartwright, commander, U.S. Strategic Command, also acknowledged: "The danger may be particularly grave if a terrorist or rogue nation can arm such missiles with nuclear warheads or other highly destructive weapons. [10]

It is notable many radical and terrorist groups add the threat of the use of nuclear weapons to their manifestos and pronouncements posted on the Internet. [11] Recent assessments indicate chemical, biological, radiological and nuclear (CBRN) "capabilities will continue to be sought by jihadist groups." [12] As a result, according

(Asymmetrical Threats, page 38)

Asymmetrical Threats … from page 5

to the National Strategy for Combating Terrorism, “Preventing their acquisition and the dire consequences of their use is a key priority.”[13]

The knowledge and resources necessary to manufacture biological and chemical agents are within the capabilities of some individuals and terrorist groups. A variety of groups seek to employ chemical agents, as was aptly demonstrated in the Sarin gas attack on the Tokyo subway in March 1995 by members of the religious group Aum Shinrikyo. In five coordinated attacks, the conspirators released Sarin gas on several lines of the Tokyo Subway, killing 12 people and seriously injuring 54. Prior to the attacks, Aum Shinrikyo extensively used video products as a means to convey various types of information to followers. [14] Consequently, this group was able to recruit followers and promulgate their sect dogma to individuals who otherwise would not have been introduced to it.

Asymmetric threats also come in the form of missiles, both short-range and ballistic, as noted by GEN Cartwright: “The most likely threats may come from adversaries that lack the traditional military apparatus of the former Cold War rivals, but nonetheless wield potentially great power with a small number of short- or medium-range missiles.”[15] As an example, during the recent military conflict in northern Israel and southern Lebanon, fighters affiliated with the radical Islamic group Hezbollah fired an average of 150 Katyusha rockets a day, more than 4,000 total, against Israeli cities, towns and villages, “employing them as political, economic and psychological weapons.”[16]

The launch sites were often placed between buildings occupied by civilians and therefore difficult to detect. The short-range rockets reached targets in seconds, making interception nearly impossible. As a result, Hezbollah forces were able to “set up a missile launcher with a couple of soldiers, move them away from the launcher and then fire it by remote control. When the Israeli retaliation hits, the Hezbollah fighters are well out of range.”[17] Significantly, the missile launchers were placed in areas where the Israeli military response, if launched by missiles or artillery fire, despite significant precautions, risked causing civilian casualties and damage to civilian infrastructure. Hezbollah exerted great effort in publicizing to the world via the Internet and other means of media dissemination the unfortunate instances of collateral damage. The employment of missiles in this manner was an example of high-visibility asymmetric attack that could be exploited through Information Operations. Moreover, the capabilities extended by the Internet have significantly increased the speed and extent of this dissemination. As acknowledged by one senior Israeli official, “When we look at the big picture, what you have is a completely different kind of war. This is asymmetric war in its purest form.”[18]

Additional asymmetric threats are posed by man-portable air defense systems. Shoulder-fired missiles have been used in at least 36 attacks on civilian aircraft in the past 30 years. In late November 2002, two shoulder-fired missiles narrowly missed an Israeli jetliner as it left the Mombasa international airport in Kenya bound for Tel Aviv. A year later, a DHL cargo plane was badly damaged after being struck by a missile in Iraq. [19] A videotape released a few days after the DHL plane attack purported to show a man firing what appeared to be a Soviet surface-to-air missile followed by a damaged cargo plane landing at Baghdad’s airport. Later analysis of the video brought into question the relationship of these purportedly connected events. However, the primary goal of the video likely had already been achieved since significantly fewer individuals became aware of the dubious validity of the video than saw the initial news report and videotape presentation.

The Cyber World Challenge

Adversaries need not invest in conventional weapons, ballistic missiles or technological alliances to acquire destructive capabilities. America’s global economy, relatively open borders and open communication sources allow access to a range of goods, services and information that together can be developed into formidable weapons. Access to knowledge, skills and components has changed significantly: “In today’s increasingly market-driven, global economy, nations so motivated have faster, cheaper and more efficient access to modern technology.”[20] Open accessibility to technological information many times through the Internet has helped lower development times and costs from both technical and budget obstacles to advanced technologies.

Notably, the Internet offers:[21]

- easy access;
- little or no regulation, censorship or other forms of government control;
- potentially huge audiences spread throughout the world;
- anonymity of communication;
- fast flow of information;
- inexpensive development and maintenance of a Web presence;
- a multimedia environment (the ability to combine text, graphics, audio and video and let users download films, songs, books, posters and so forth);
- the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories.

Adversaries have found unexpected ways to use familiar technology against us. Even low-tech countermeasures can exploit the vulnerabilities of some U.S. weapons and their supporting systems. Cyber-attacks can be used to disable computer networks, paralyzing communications, transportation, power systems and industrial enterprises. Our nation’s reliance on automated systems for its critical infrastructure, including energy distribution, transportation,

For years, disturbing videos of executions, ambushes and roadside bombings have been disseminated to interested audiences. However, the emerging trend is how these videos are distributed. The dissemination of videos on the Internet showing the murders of the journalist Daniel Pearl in Pakistan and the American businessman Nicolas Berg in Iraq resulted in extensive renown for the perpetrators but shock and condemnation from the civilized world at large.

banking and finance, emergency services, telecommunications and continuity of government, makes their disruption potentially devastating.[22] Notably, societies with immature information assurance systems may be at even greater risk to cyber-attacks.

The great virtues of the Internet — ease of access, lack of regulation, vast potential audiences and fast flow of information — are also being widely used by groups committed to asymmetric warfare. By its very nature, the Internet is an ideal environment for use by groups that want to exchange or disseminate information with current and potential supporters. Notably, "adversaries are increasingly exploring and testing Information Operations actions as asymmetric warfare that can be used to thwart U.S. military objectives that are heavily reliant on information systems. This requires the U.S. military to employ defensive technologies and utilize leading-edge tactics and procedures to prevent our forces and systems from being successfully attacked."[23]

Contemporary adversaries use the Internet in a variety of ways, including: developing and disseminating propaganda, raising and transferring funds, recruiting, data mining and coordination of attacks. As noted in the National Strategy for Combating Terrorism: "The Internet provides an inexpensive, anonymous, geographically unbounded and largely unregulated virtual haven for terrorists. Terrorist organizations can use virtual safe havens based anywhere in the world, regardless of where their members or operatives are located."[24] This same description applies to the use of the Internet by our Nation's adversaries who have not been described as "terrorists."

One of the most important ways in which adversaries use the Internet is as a medium for propaganda. Until the advent of the Internet, many groups' hopes of winning publicity for their causes and activities depended on attracting the attention of television, radio or the print media. For years, disturbing videos of executions, ambushes and roadside bombings have been disseminated to interested audiences. However, the emerging trend is how these videos are distributed. The dissemination of videos on the Internet showing the murders of the journalist Daniel Pearl in Pakistan and the American businessman Nicolas Berg in Iraq resulted in extensive renown for the perpetrators but shock and condemnation from the civilized world at large. More recently, the posting of a video clip on the CNN Web site purportedly showing sniper attacks on Americans Soldiers was apparently made by Iraqi insurgents with the intent of influencing the American public as well as rallying supporters.[25] The expeditious transmittal of images to worldwide audiences will likely increase in the future: "The cellular [networks] and land lines have become ingredients of the modern psychological and propaganda wars, joining other tools … like the radio, TV, flyers and the Internet."[26]

U.S. intelligence sources cite some 30 nations that have developed aggressive computer warfare programs; however, relatively few countries currently have the extensive technical and financial resources to mount sophisticated attacks on U.S. weapon systems and computer networks.[27] Nevertheless, denial of service attacks, cyber-incursions and malicious attempts to adversely affect physical infrastructures like power grids and banking transactions have increased in frequency and sophistication in the past few years. As a point of comparison, the number of reported attempts to penetrate computer networks supporting the Pentagon has risen from fewer than 800 in 1996 to more than 160,000 in 2005.[28] Similarly, computer-related crime is having an increased financial impact. The Federal Bureau of Investigation estimates all types of computer crime in the U.S. has already cost industry approximately $400 billion.[29] Of equal concern is the unauthorized theft of information and identities. Spyware software, in particular, is a pervasive problem, both for individuals and organizations. By one estimate reported in August 2006, some 527,000 malicious Web sites were identified, an increase of 100,000 from just a year earlier.[30]

Direct attacks have been made against individual Web sites, although these actions have generally been limited in both scope and importance. In one of the most widely reported instances, a variety of would-be cyber-terrorists swore to carry out a "revenge battle on Danish newspapers" in retaliation for publication of cartoons of the Prophet Muhammad in September 2005.[31]

Supporting the Fight in the Information Environment: The Role of the Space Professional

The challenge today for commanders is to operate effectively in dynamic joint and multinational operational environments while combating a tenacious and capable enemy. Information superiority is vital to this process. Very simply, "the goal of Information Operations is to gain and maintain information superiority, a condition that allows commanders to seize, retain and exploit the initiative. Information Operations involves constant efforts to deny adversaries the ability to detect and respond to friendly operations, while simultaneously retaining and enhancing friendly force freedom of action."[32] Information Operations supports the collection and processing of battlefield information into actionable information, which then supports achievement of mission objectives designated by the commander. This relationship is particularly important in insurgent and asymmetric environments. Winning against a determined enemy requires that we operate at a faster tempo than our adversaries, or better, get inside his decision-making process.

Space professionals must consider that Information Operations is conducted within the context of an environment — an Information Environment. This Information Environment is comprised of physical, informational and cognitive dimensions that interrelate as individuals, organizations and systems.[33] Consequently, a thorough Intelligence Preparation of the Battlefield is required to fully assess the breadth and relationships between the three dimensions.

The physical dimension is comprised of the command and control systems and supporting systems (physical platforms and the communications networks) that enable individuals and organizations to conduct operations across the domains of air, land, sea and Space. Because information enhances capabilities, the resources required to maintain this dominance provide lucrative targets for asymmetric threats. As new technologies develop, so too will be the means and approaches of attack and disruption. As a result, this dimension must be protected from physical attack.

The informational dimension is where information is collected, processed, stored, disseminated, displayed and protected. This information is generally accessible to the world at large. It is also the dimension where the command and control of military forces is communicated.

The cognitive dimension is where decision-makers and the target audience think, perceive, visualize and decide. A leader's ability to recognize what is happening and remain attentive to threats, change and opportunity is one of the most difficult challenges of asymmetric warfare. The factors of leadership, morale, unit cohesion, level of training, experience, situational awareness, as well as public opinion, media, local attitudes and personalities of those living in the area of operations influence this dimension. As indicated in a recent article, "Winning … is as much about winning the trust and confidence of the people … as it is about winning tactical battles on the ground."[34] This dimension also includes enemy capabilities, decision-making styles and what information systems the enemy has at their disposal.

In planning Information Operations support for commanders, Space professionals have multiple U.S. Army Space and Missile Defense Command/U.S. Army Forces Strategic Command organizations at their availability. All of these assets must be considered when planning support, particularly against asymmetric threats. Space-based capabilities, for example U.S. Strategic Command's Measurement and Signature Intelligence Advanced Geospatial Intelligence (MASINT AGI) Node, supports decision superiority in the informational dimension through the provision of commercial and civil data from satellite, ground and airborne sources. The 53rd Signal Battalion (Satellite Control) supports the provision of satellite communications to convey Information Operation products. The Joint Blue Force Situational Awareness Mission Management Center provides blue force situational awareness data to the Common Operational Picture to support situational awareness.

Space professionals also must continually consider steps to protect the informational dimension of friendly forces from cyber-attack. Concurrently, they must be prepared to provide technical advice to commanders on how to deny adversaries access to their own communications and media links and nodes. For example, Space Control capabilities could deny the provision of position, navigation and timing data for which to support adversaries' decision-making.

The Unexpected Can Always Happen

In a recent magazine article, GEN Cartwright wrote, "Americans are familiar with the host of new challenges posed by the forces of international terrorism, but one of the greatest threats we face may not be human at all … the next big threat could be a natural disaster or something unanticipated."[35] The article went on to emphasize the importance of putting in place the fundamental structures to address challenges and threats wherever they might originate. Military actions often have second- and third-order effects and the opportunity for unintended consequences increases with uncertainty and asymmetry. Consequently, Information Operations is not likely to be a short-lived operational planning requirement. Space professionals must be at the center of the planning process, and should be prepared to consider the implications of the following questions: [36]

- How do we counter a threat that seeks to obviate the advantages we possess in conventional military power?
- How might our enemy change his operational structure or organization in an attempt to accomplish his ends?
- In what areas might he develop superior knowledge or some unprecedented use of a capability?
- What capabilities do our adversaries have that we do not understand or expect?
- How do we anticipate their ability to innovate?

Former Secretary of Defense Donald Rumsfeld recently emphasized: "The future will require us to think differently and develop the kinds of forces and capabilities that can adapt quickly to new challenges and unexpected circumstances." [37] In considering the challenges of countering adversaries employing asymmetric approaches, we must remember that borders have become seamless. Moreover, adversaries are increasingly becoming more adept at combining conventional capabilities with cyber-world media suaveness. In response, Space professionals must be prepared to step forward and leverage our Nation's great technological capabilities in support of joint warfighters.

Secure the High Ground!

REFERENCES

1. Fact Sheet, Combating Terrorism: Presidential Decision Directive 62, May 22, 1998, online at <http://www.fas.org/irp/offdocs/pdd-62.htm>, accessed Oct. 24, 2006.

2. Joint Publication 3-13, Information Operations, Feb. 13, 2006, pg. GL-9; online at <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>, accessed Oct. 15, 2006.

3. LTC LaWarren V. Patterson, "Information Operations and Asymmetric Warfare…Are We Ready?" U.S. Army War College Strategy Research Project, online at <http://www.iwar.org.uk/iwar/resources/asymmetric-io/Patterson_L_V_02.pdf>, accessed Oct. 3, 2006.

4. COL (retired) Clinton J. Ancker III and Lieutenant Colonel (retired) Michael D. Burke, "Doctrine for Asymmetric Warfare;" Military Review, July-August 2003, pg. 24, online at <http://www.au.af.mil/au/awc/awcgate/milreview/ancker.pdf>, accessed Sept. 8, 2006.

5. Steven Lambakis, James Kiras, Kristin Kolet, "Understanding "Asymmetric" Threats to the to the United States;" National Institute for Public Policy, September 2002, pp. 19-20, online at <http://www.nipp.org/Adobe/Asymmetry%20%20final%2002.pdf>, accessed Sept. 10, 2006.

6. GEN (retired) Montgomery C. Meigs, cited in "Army Faces Rising Number of Roadside Bombs in Iraq," Ann Scott Tyson, Washington Post, Sept. 8, 2006, pg. A-12, online at <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/07/AR2006090701372.html>, accessed Sept. 8, 2006.

7. William S. Lind, "Operational IEDs," online at <http://d-n-i.net/lind/lind_12_01_05.htm>, accessed Sept. 28, 2006.

8. Edward Wyatt, "Anti-U.S. Attack Videos Spread on Web," online at <http://www.nytimes.com/2006/10/06/technology/06tube.html?pagewanted=1&ei=5070&en=87298d2da43cf30b&ex=1161403200>, accessed Oct. 6, 2006.

9. Quadrennial Defense Review Report; Feb. 6, 2006; online at <http://www.comw.org/qdr/06qdr.html>, accessed March 10, 2006.

10. Elaine M. Grossman, "Cartwright: U.S., Russia Mulling Security Options Amid Spread in Arms," Inside the Pentagon, Aug. 10, 2006, reprinted in USASMDC/ARSTRAT News Clips, Aug. 10, 2006.

11. Steve Coll, "What Bin Laden Sees in Hiroshima," The Washington Post, Feb. 6, 2005, page B01, online at <http://www.washingtonpost.com/ac2/wp-dyn/A365-2005Feb5?language=printer>, accessed Feb. 6, 2005.

12. Declassified Key Judgments of the National Intelligence Estimate. Trends in Global Terrorism: Implications for the United States, dated April 2006, online at <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/26/AR2006092600163.html>, accessed Sept. 27, 2006 and Joby Warrick, "Suspect and A Setback in Al-Qaeda Anthrax Case," The Washington Post, Oct. 31, 2006; page 1, online at <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/30/AR2006103001250.html>, accessed Oct. 31, 2006.

13. National Strategy for Combating Terrorism, pg. 12, online at <http://www.whitehouse.gov/nsc/nsct/2006/nsct2006.pdf>, accessed Oct. 5, 2006.

14. Yomiuri Shimbun, "Day of Judgment: Teachings of Guru Still Drive Aum," Feb. 24, 2004, online at <http://www.religionnewsblog.com/6186/day-of-judgment-teachings-of-guru-still-drive-aum>, accessed Oct. 18, 2006.

15. Grossman.

16. Andrew McGregor, "Hezbollah's Rocket Strategy," TerrorismMonitor, Volume 4, Issue 16, Aug. 10, 2006, online at <http://jamestown.org/terrorism/news/article.php?articleid=2370098>, accessed Aug. 11, 2006.

17. Greg Sheridan, "It's a new way of war and we'd better get used to it," The Australian, Aug. 10, 2006, online at <http://www.theaustralian.news.com.au/story/0,20867,20074229-25377,00.html>, accessed Sept. 18, 2006.

18. Scott Wilson, "Missile War is a New Challenge to Israel's Long Rule of the Sky," July 19, 2006, online at <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/18/AR2006071801387.html>, accessed July 19, 2006.

19. Del Quentin Wilber, "Police on the Lookout for Terrorists with Missiles near Airports," Sept. 9, 2006, online at <http://www.washingtonpost.com/wp-dyn/content/article/2006/09/08/AR2006090801451.html>, accessed Sept. 9, 2006.

20. Lambakis, Kiras, Kolet, pg. 12.

21. Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace, online at <http://www.usip.org/pubs/specialreports/sr116.pdf>, accessed Sept. 15, 2006.

22. Jonathan B. Tucker, "Asymmetric Warfare," online at <http://forum.ra.utk.edu/1999summer/asymmetric.htm>, accessed Sept. 14, 2006.

23. Joint Publication 3-13, pg. I-11.

24. National Strategy for Combating Terrorism,
pg. 17.

25. "Video Shows Snipers' Chilling Work in Iraq," Oct. 19, 2006; online at <http://www.cnn.com/2006/WORLD/meast/10/19/iraq.sniper.video/index.html>, accessed Oct. 19, 2006.

26. Donna Abu-Nasr, "Israel Fights Propaganda War Over Phones," Aug. 7, 2006, online at <http://www.jpost.com/servlet/Satellite?pagename=JPost%2FJPArticle%2FShowFull&cid=1154525824340<, accessed on Aug. 18, 2006.

27. Patterson, pg. 4.

28. "Hacker Attacks Hitting Pentagon," Siobhan Gorman, Baltimoresunl.com, July 2, 2006, online at <http://www.networksecurityarchive.org/html/Information-Security-News/2006-07/msg00148.html>, accessed Oct. 24, 2006.

29. Mathew Jones, "Cyber-Crime Becoming More Organized," Reuters; Sept. 15, 2006; online at <http://www.eweek.com/print_article2/0,1217,a=188746,00.asp>, accessed Oct. 2, 2006.

30. Arik Hesseldahl, "Social-networking sites a "hotbed" for spyware," BusinessWeek Online, Aug. 18 2006; online at <http://msnbc.msn.com/id/14413906/print/1/displaymode/1098>, accessed Oct. 2, 2006.

31. Evan F. Kohlmann, "The Real Online Terrorist Threat," pg. 121, online at <http://www.foreignaffairs.org/20060901faessay85510/evan-f-kohlmann/the-real-online-terrorist-threat.html>, accessed Oct. 3, 2006.

32. Field Manual 3-13; Information Operations: Doctrine, Tactics, Techniques, and Procedures; Nov. 28, 2003; pg. v; online at <http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf>, accessed Oct. 18, 2006.

33. Joint Publication 3-13, pp. I-1 and I-2.

34. LTC Pamela Keaton and MAJ Mark McCann, "Information Operations, STRATCOM, and Public Affairs," pg. 84, online at <http://usacac.leavenworth.army.mil/CAC/milreview/download/English/NovDec05/keeton.pdf>, accessed Oct. 30, 2006.

35. GEN James Cartwright, "Information Sharing Is a Strategic Imperative," Crosstalk, the Journal of Defense Software Engineering, July 2006, online at <http://www.stsc.hill.af.mil/CrossTalk/2006/07/0607Cartwright.html>, accessed Oct. 22, 2006.

36. Montgomery C. Meigs, "Thoughts About Asymmetric Warfare," Parameters, online at <http://www.carlisle.army.mil/USAWC/Parameters/03summer/meigs.pdf>, accessed Sept. 10, 2006.

37. Thomas J. Williams, "Strategic Leader Readiness and Competencies for Asymmetric Warfare," Parameters, online at <http://www.carlisle.army.mil/USAWC/parameters/03summer/williams.pdf>, accessed Sept. 15, 2006.