

**STRATEGIC CHALLENGES FOR COUNTERINSURGENCY
AND THE GLOBAL WAR ON TERRORISM**

**Edited by
Williamson Murray**

September 2006

This publication is a work of the U.S. Government as defined in Title 17, United States Code, section 101. As such, it is in the public domain, and under the provisions of Title 17, United States Code, Section 105, it may not be copyrighted.

Visit our website for other free publication downloads

<http://www.StrategicStudiesInstitute.army.mil/>

[To rate this publication click here.](#)

The views expressed in this report are those of the authors and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244.

All Strategic Studies Institute (SSI) monographs are available on the SSI homepage for electronic dissemination. Hard copies of this report also may be ordered from our homepage. SSI's homepage address is: *www.StrategicStudiesInstitute.army.mil*.

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on our homepage at *www.StrategicStudiesInstitute.army.mil/newsletter/*.

ISBN 1-58487-247-0

CHAPTER 11

THE DARK FRUIT OF GLOBALIZATION: HOSTILE USE OF THE INTERNET

Lieutenant Colonel Todd A. Megill

One of the second order effects of an internet connected world, a direct consequence of increasing economic globalization and technological diffusion, is that insurgent/terrorist organizations which are most against the process of globalization are using its infrastructure to target and attack its biggest proponent, the United States. As the world's greatest power and leading engine of change, the United States has created through the internet a "virtual global commons," one that anti-American and anti-globalization groups increasingly are using to conduct propaganda and plan attacks. This chapter will focus on the internet, developed as an agent of economic change, and its use by insurgents/terrorists to operate and conduct targeting operations employing a similar methodology adopted by the U.S. Department of Defense (DoD).

U.S. National Security, Economic Prosperity, and the Internet.

One of the major goals of the current U.S. National Security Strategy is to create and expand the world economy as a means for addressing some of the underlying causes of violence around the globe:¹

A Strong World Economy enhances our national security by advancing prosperity and freedom in the rest of the world. Economic growth supported by free trade and free markets creates new jobs and higher incomes. It allows people to lift their lives out of poverty, spurs economic and legal reform, and the fight against corruption, and it reinforces the habits of liberty.²

Creating a strong world economy will lead the United States even more toward embracing the concept and trends of globalization: "Globalization refers to those entrenched and enduring patterns

of worldwide interconnectiveness . . . it suggests that a growing magnitude or intensity of global flows such as that the states and societies become increasingly enmeshed in worldwide systems and networks of interaction."³ The process of globalization, though initially created by U.S. technical creativity and economic power, is now truly a world-wide phenomenon as millions around the world contribute their expertise, creativity, and economic capital.

Globalization isn't a choice. It's a reality. There is just one global market today, and the only way you can grow at the speed your people want is by tapping into the global stock and bond markets, by seeking out multinationals to invest in your country and by selling into the global trading system what your factories produce. And the most basic truth about globalization is this: No one is in charge – not George Soros, not 'Great Powers' and not I.⁴

Technological advances in telecommunications and computerization leading to the creation of the internet are the leading characteristics of the process involved in globalization. "Today's era of globalization is built around falling telecommunication costs—thanks to microchips, satellites, fiber optics, and the internet."⁵ If the global movement of goods and services are the lifeblood of the world economy, then the internet is the nervous system. It is constantly passing, collecting, and storing information that guides and directs such economic flows. The movement of information and data across the internet is so vast and pervasive in the United States, and the industrialized world in particular, that it has become a feature of modern life. Air travel, sea travel, land travel, and now virtual travel that cross these global commons are the norm. A commons represents a shared resource or area with poorly defined boundaries, widely used or accessible, with limited supervision or governance. The last form of travel has no association with geography, possesses no boundaries, and is limited only by access to the World Wide Web. The internet is a continually expanding virtual commons of information and communication stretching across the globe.

The Impact of a Virtual Global Commons.

The major impact of the internet is that it has evolved into the fourth global commons. There is a terrestrial commons of land

masses, an oceanic global commons that encompasses most of the globe, and an aerospace global commons that covers the earth and extends upward until the atmosphere ends in empty space.⁶ The internet has created a virtual global commons that extends as far as communications can reach and man has a desire to create an interface.

The virtual global commons that the internet provides for hostile users is unique and expands the opportunities for insurgency, criminality, terrorism, or other violent acts across the globe. There is little common agreement on the terms of terrorism or insurgency or if the current wave of Muslim fundamentalist extremism is a political movement linked to an insurgency or random terrorist acts.⁷ The use of the internet for violence does not predispose any political goal or objective, and so the term terrorist/insurgent is used in this discussion. The worldwide internet allows the hostile terrorist/insurgent to create and/or occupy a "Distributed Sanctuary." The U.S. Joint Chiefs of Staff defines a sanctuary as: "A nation or area near or contiguous to the combat area which by tacit agreement between the warring powers is exempt from attack and therefore serves as a refuge for staging, logistic, or other activities of the combatant powers."⁸ The worldwide internet allows an expansion of that definition. The refuge or sanctuary no longer has to be near or contiguous to the area of combat or operations.

The linkages provided by the worldwide internet allow the insurgents and terrorists to remain removed from the location they plan to attack. "The knowledge of how to conduct an attack is developed in one country, then that knowledge is combined with the raw materials, personnel, and training available in other countries, which can include the target country, to create a weapon in the target country."⁹ Options now exist to divide a sanctuary further, not only by location, but by function.

The world-wide internet allows an organization's fund raising to occur around the globe and its collection to occur in a country that looks favorably upon terrorist or insurgent goals. "Al-Qa'ida appears to have relied on a core group of financial facilitators who raised money from a variety of donors and other fund-raisers, primarily in the Gulf countries and particularly in Saudi Arabia."¹⁰ Terrorists and insurgents use existing legal and illegal networks to gain financing

including the use of free trade zones and the informal hawala system of currency transfers, including diamonds and gold.¹¹ The monies sent to those who are planning operations in another location or a nation-state, to locations with weak banking and financial laws, allows them to launder the monies collected.

Money laundering involves disguising assets so they can be used without detection of the illegal activity that produced them. . . . This process has devastating social consequences. For one thing, money laundering provides the fuel for drug dealers, terrorists, arms dealers, and other criminals to operate and expand their operations.¹²

Insurgents and terrorists can reside in a country where they are breaking no public laws and can maintain a low profile. In a second country or location, other members procure and assemble the weapons or explosives for shipment to marry up with the actual attackers in yet a third country or location. The terrorists and insurgents attackers can then flee or return to possibly a fourth country, the operation monitored by the group's leadership using news outlets and media access from yet another country. Finally, the terrorists and insurgents can develop the group's message and disseminate it throughout the world through the world-wide internet. Separating the various functions of insurgent and terrorist sustainment and operations or the phases of the targeting and attack methodology makes it difficult for national police or public security organizations to track and/or gather evidence of criminal misconduct. "The old police technique of tracking illegal activity by watching certain places and peoples does not work when communications is carried out on line."¹³

As we now know, support networks in Muslim diasporas, especially in Europe, have been key nodes in the funding and operations of extremist and terrorist groups. Ironically, the activities of these groups have been facilitated by the reluctance of Western security and law enforcement agencies to monitor the activities of allegedly religious groups. As the investigations following the events of September 11, 2001 have run their course, it has become apparent that Muslim diasporas in countries such as Germany, the United Kingdom, France, Spain, Belgium, and Switzerland have been implicated as important hubs of al-Qa'ida operations and recruitment.¹⁴

One of the challenges the worldwide internet poses as a global commons is that it already exists as an exploitable environment. It has the ability to be present or embedded into every aspect of mankind's existence. Thus, insurgents and terrorists do not have to expend much time, effort, or money to painfully build up the infrastructure for attack or revolt. The painstaking process of building cells, organizations, and networks and the risks of communicating with them greatly decrease when done remotely. "Even more challenging from a security point of view is that the people do not have to go out to establish these networks. They do not have to be in the same country or even on line at the same time."¹⁵

The internet is such a useful communications and economic tool that it is unlikely that a modern society can operate without it. The world economy, linked through a global communications network, has helped raise the standard of living of millions around the world.¹⁶ However, this communications infrastructure also brings change to much of the world. For those who do not want change and seek to deny it, the internet can become a tool for attacking the very bodies, values, and organizations that helped to create it.¹⁷ The Internet allows for a criminal, an insurgent, or a terrorist to expand his or her area of operations and gather the necessary information about targets they wish to exploit or attack without a physical presence until the actual tactical operation occurs.

Doctrine: Ours and Theirs.

In the U.S. military, at the Joint level, Joint Pub 3-60, *Joint Doctrine for Targeting*, dated January 17, 2002, promulgates the doctrinal underpinnings of the targeting process.¹⁸ The six-step process is used to define targets for attack in support of combat operations: (1) Commander's objectives, guidance and intent, (2) Target development, validation, nomination, and prioritization, (3) Capabilities analysis, (4) Commander's decision and force assignment, (5) Mission planning and force execution, and (6) Combat assessment. Within this process, the U.S. Army and Marine Corps use the Decide, Detect, Deliver, and Assess Cycle (D3A) to support planning and link with the Joint Targeting Cycle (see Figure 1).¹⁹

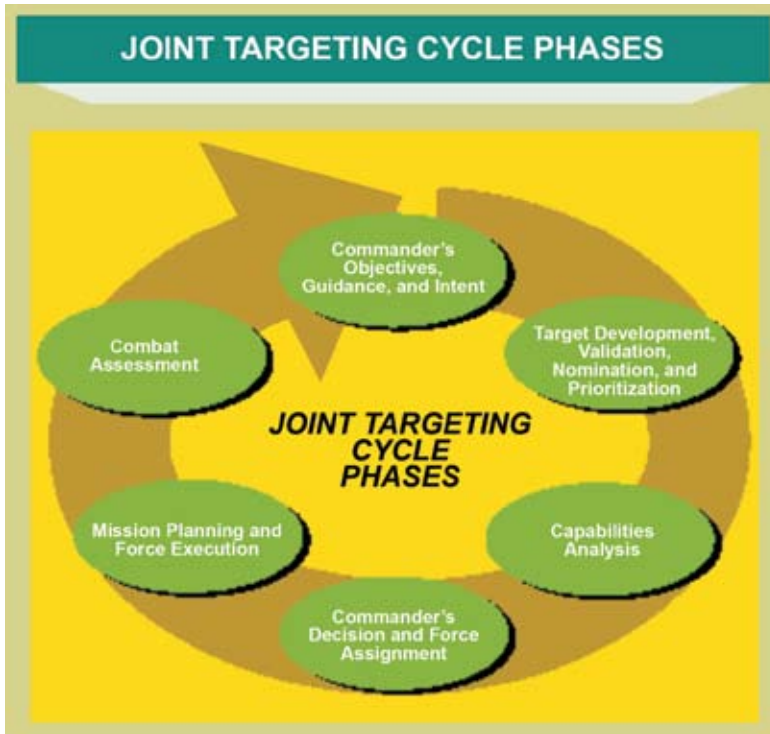


Figure 1. The Joint Targeting Cycle.

This methodology is similar in many ways to the type of process that insurgents or terrorists use in defining, developing, and executing their attacks.²⁰ Moreover, the interconnectiveness of modern society and the presence of the internet allow the insurgents/terrorists to accomplish many of these steps from a distributed sanctuary, removed from the actual geographic location or population they intend to attack.

Commander's Objectives, Guidance, and Intent.

In both the U.S. military and insurgent or terrorist organizations, there are policy objectives achieved by the application of force or the threat of force. Both organizations provide this guidance and intent to subordinates in different forms: written documents, oral presentations, conversations, and graphics, stories, and pictures.²¹ The internet makes this important step easier, as it allows those physically separated to maintain a high level of contact and communication.

There used to be trade-off, they argue, between the reach of a message and its richness. A rich, detailed message required a one-on-one conversation; reaching out to thousands, for example, through advertising, meant you could send only simplistic messages. The tradeoff has now been killed by the new technologies: you can have rich, detailed customized information flowing from one to thousands or millions.²²

The internet allows the communication of a leader's or commander's intent and guidance to his or her subordinates accurately, without the risk of actual physical contact that could lead to identification, arrest, or attack.

Target Development, Validation, Nomination, and Prioritization; and Capabilities Analysis.

This is the step that involves target selection. The U.S. Army's decide phase in the D3A Cycle is embedded in this, as military personnel decide what are the type of targets, where they are, who can locate them, and how they should be attacked.²³ This is a give-and-take process between intelligence and operations functions. A process that debates, assembles, and selects targets for lethal or nonlethal attack. Additionally, the evaluation and selection of the target results in the identification of the type of attack system or methodology likely employed against the nominated target. Again, the internet allows the insurgent/terrorist a similar capacity to communicate accurately over vast distances and keep track of individuals, ideas, and targets. The internet is an interconnected assemblage of databases that provides the insurgents/terrorists a low-cost, low-risk way of gathering information about their enemies. The Al-Qa'ida organization, a recent example of an evolving insurgent/terrorist network, uses computers and the internet as a matter of course to operate their organization and identify targets.

Al-Qa'ida was a modern army. It was as adept with computers as any organization, founded by the engineer son of a construction millionaire and staffed largely by middle-class educated males. Intercepting al-Qa'ida communications was hard mainly because the organization understood information technology so well.²⁴

Expertise with information technology and the internet allows the insurgents or terrorists to gather the information needed to conduct their planning, targeting, and weaponeering remotely:

Meanwhile, al-Qa'ida operatives used the Internet to scope out targets. They downloaded layouts of bridges and buildings from Web sites. In the past, collecting this kind of information might require traveling around the world. Getting it to someone in the field required undercover couriers. Now you could click, get the data, click again, and send the diagrams to a temporary, untraceable e-mail address.²⁵

A translation of an al-Qa'ida Training manual gives clear guidance to followers and operatives on how to gather information and intelligence about an enemy or target:

Any organization that desires to raise the flag of Islam high and proud must gather as much information as possible about the enemy. Information has two sources: Public Sources: Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of the information available about the enemy. . . . The one gathering the information should be a regular person (trained college graduate) who examines primary sources of information published by the enemy (newspapers, magazines, radio, TV, etc.). . . . The one gathering information with this public method is not exposed to any danger whatsoever. Any brother can gather information from those aforementioned sources.²⁶

The internet makes it possible for a global insurgency or terrorist networked organization to exist. Prior to the invention and dissemination of the internet, geography had a great influence on the movement of information. The physical distance between members made communications and information collection much slower, riskier, and more time consuming.

Commander's Decision and Force Assignment; and Mission Planning and Force Execution.

These two phases are intertwined so closely that they can occur nearly simultaneously. Now the commander approves selected targets, which are then attacked. In U.S. Army doctrine, this is the

deliver phase of the Joint Targeting Cycle. The U.S. military and insurgents and terrorists have a number of ways of attacking the target(s), but the U.S. military has the advantage in possessing specialized weapons that can afford it considerable target standoff and destructive power. Insurgents and terrorists on the other hand currently have neither standoff nor destructive capability, but they possess their own considerable capability.

The advance of technology is why we now worry about weapons of mass destruction. For the first time in history, a single attacker may be able to use technology to kill millions of people. . . . Technology will continue to alter the balance between the attacker and the defender, at an ever-increasing pace. In addition, technology will generally favor the attacker, with the defender playing catch-up.²⁷

The U.S. President has stated in the National Security Strategy, "The gravest danger our Nation faces lies at the crossroads of radicalism and technology."²⁸ The internet can serve as a command, control, communications, computerization, and intelligence center to facilitate lethal attacks. In addition, there is a growing body of literature that indicates it could be the actual attack mechanism to disable or disrupt certain components of a modern industrialized society.²⁹ Again, the insurgent/terrorist need not be physically present in relation to the target when conducting such an attack.

Combat Assessment.

The Joint Targeting Process's final phase, mirrored in the U.S. Army's cycle, is the assessment phase. This represents the estimate of the damage resulting from the use of force.³⁰ The U.S. military uses intelligence and operational assets to evaluate the damage to the target and assess if it has achieved the commander's desired level of effect. If the needed level of effect is not adequate, then the target is attacked again. Insurgents or terrorists evaluate a target they have attacked in relation to its symbolic and propaganda value. The internet greatly facilitates such an evaluation as it grants nearly real-time knowledge of the attack and target impact due to the presence of the world media. An insurgent or terrorist attack is big news in most

of the world, and the immediate broadcasts of images of the attack help terrorists and insurgents evaluate their success. In a crude way, the sheer amount of reporting on a given attack provides insurgents and terrorists with an idea of how successful the organization's attack has been. Monitoring multiple media outlets from around the world is easy to do on the internet. It allows the insurgents or terrorists to monitor their attack at the same time they advertise their activities and promote their views and cause. This then completes the targeting process with the organization's message being enhanced or modified. The targeting process begins again with insurgents or terrorists looking for new targets to attack. The internet allows this targeting process to occur across the globe with the insurgent/terrorist network being connected by the thinnest web of electrons through the internet.

Conclusion.

The expanding use of the internet lies at the heart of the globalizing world economy. The interconnectiveness of the financial and business sectors around the world is critical to the quality of life and standard of living of Americans. The United States, in an effort to improve its national security posture, actively promotes the global economy as a way to address numerous social evils and promote basic human rights.³¹ The internet is a means of more firmly integrating all nations of the world into more interconnected and stable political units. This allows increased efficiencies that translate into economic improvements. However, the internet brings both opportunities and threats. It is a method of improving efficiencies and linkages between people and businesses. It also serves as a tool for those opposed to the globalized political economy and allows them to tap into the fears of dynamic change. Thus, they can carry on a networked anti-American insurgency.

The targeting methodology that the U.S. military uses at the joint level is similar at both the operational/strategic and tactical levels to how global insurgents and terrorists can now conduct their own operations using the internet. The ability to send clear, concise, information dense messages across the world enhances the

insurgents' security. They no longer have to meet face-to-face to encourage members or develop plans. The internet allows individuals and small groups with common agendas to make and maintain contact easily with each other. The internet serves as a global venue to disseminate their message or vision. The internet not only provides a highly effective means of organizing, commanding, and controlling an insurgent or terrorist network, but also serves as a useful tool to collect targeting information. Terrorists or insurgents can conduct operational planning, target evaluation, initial weaponeering, and a post-attack assessment without physically visiting the intended target. This remote targeting process, buried in the mass of traffic and data that flows across the World Wide Web, makes it difficult for security forces to track insurgent/terrorist activities. The internet allows the insurgents or terrorists to expose themselves to a minimal amount of risk of capture until the actual execution of the targeted attack. After attacking the target, the organization can monitor its success nearly instantaneously at almost no cost or risk to itself. Finally, the internet allows the insurgents and terrorists to trumpet their activities when they chose to do so throughout the world, again both quickly and with relative security.

The internet allows the establishment of a worldwide insurgency by non-state actors. Empowered angry young men can link themselves together via the internet and become a cohesive organization, networked together.³² Insurgents or terrorists seldom need to come together to maintain a functional organization. The internet allows insurgents and terrorists to remain scattered across the globe and hidden in small groups. They need not come together to operate, creating a difficult signature for security officials to find. The internet is a growing virtual global commons that affords small numbers of violent individuals the opportunity and capability to carry out a global insurgency and complex, devastating attacks. Thus, the expansion of the internet, linked to economic prosperity, is a two-edged sword, improving people's standard of living, while at the same time empowering those in violent disagreement with the values and concepts it embodies to attack its proponents more effectively.

Recommendations.

The internet is here to stay as a major component of the world's economic system and a highly visible presence in the process of globalization. The internet's rapid growth and penetration into all aspects of the industrialized and developing world has led it to become a part of a new "Virtual Global Commons." Since the internet is now an integral part of world civilization and has the nature of open access, there is no way to deny its use to insurgents or terrorists for their own criminal and violent agendas. Denying the internet as a distributed sanctuary is an impossibility for the United States. Attempting to cut the insurgents or terrorists off from the internet and its networks, would display a complete lack of understanding of its capabilities and operation. A quote from an earlier era illuminates the challenge to the United States in combating insurgents and terrorists on the internet.

Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand little hurt if they avoid a greater one. If you try to hold everything, you hold nothing.

Fredrick the Great³³

There should be a two-pronged approach in addressing the insurgent and terrorist threat on the internet. The first would be to manage the risk the internet possesses as an insurgent or terrorist command and control and intelligence collection tool. This is the classic concept of force protection and physical security. General information about a target is probably not deniable to insurgents or terrorists. However, the United States needs to deny the insurgents detailed information about possible targets. This is a major component of the current strategy for defending cyberspace.³⁴ The United States is doing this, and it will make the insurgents or terrorist's targeting process more difficult. In addition, the United States government needs to continue to harden its own cyber-networks to minimize any direct collection or attack on vital network infrastructures through possible interfaces with the commercial or civil internet. The insurgent and terrorist likely will use the internet as a means to launch cyberattacks against selected targets.

The second approach to addressing a hostile use of the internet is less traditional, as it would seek to exploit the insurgents or terrorists use of the internet, rather than attempt to deny them access. The internet can work for the United States military as well as for insurgents or terrorists. The latter exploit the internet, but using the internet means that they have to utilize the technology it encompasses. The U.S. Government needs to expand and enlarge the internet, adding more nodes and infrastructure. By doing so, it will attack indirectly, using economic power, the source of people's frustrations and lack of hope that are breeding grounds for insurgencies and terrorism. The expansion of the internet will make it easier to track and monitor insurgent or terrorist organizations. The use of the internet leaves an electronic record, trail, or trace. Skilled operators and analysts can trace these links back to insurgents or terrorists. The tracking information can then be turned over to more classic human intelligence or technical collection for targeting. The ability to operate dispersed also makes insurgents and terrorists more vulnerable, since they lack the situation awareness and protection that massing provides. The distributed, global nature of the internet allows the United States to conduct remote collection against insurgents/terrorists, while minimizing the risk to its service members and increasing the efficiency of more traditional intelligence collection.

Moreover, the U.S. Government needs to encourage expansion and use of the internet on a global basis in an effort to deny insurgents and terrorists access to unaccountable operational funds. The free flow of undocumented currency allows the fusion of criminals and insurgents or terrorists to finance operations and suborn individuals to provide them information and support. The increasing use of the internet as a mechanism for retail and business-to-business financial transactions not only avoids the inefficient use of hard currency, but it also allows documentation of the financial trail. Tracing the financial transactions allows their exploitation by law enforcement agencies for arrest or the U.S. Government for military targeting. The more financial transactions travel across the internet, the less the potential for undocumented currency to become available to criminal or insurgent or terrorist organizations, which would limit their ability to conduct and promote operations.

Insurgents and terrorists use the internet as a propaganda and a recruiting tool. Through websites and internet chat rooms, they put out their message in an effort to influence and recruit. Again, the internet should allow the U.S. Government to monitor this process. Its representative could then use information operations, promoting a dialog by using or hiring religious or political leaders to promote moderate viewpoints. Any communications created during this dialog would not only work to counter the insurgents or terrorists message, but also create other opportunities for active, targeted collection.

Finally, the United States, as it continues to promote globalization and seeks to transform many federal government organizations, needs to maintain a priority of monitoring and researching the internet. The relative “newness” of the internet and the distributed, nearly chaotic way in which it grows and operates, means that its capabilities and effects are poorly understood. Insurgents and terrorists are using the internet and constantly evolving their tactics and techniques. Although they have adapted their organizations to take advantage of the internet, they have not yet evolved into “networked” insurgent organizations. The United States needs to remain vigilant as networked insurgent and terrorist organizations are still in their infancy. Through observation, research, and simulation its operatives, in cooperation with the private sector, need to understand the capabilities and limitations the internet imposes on its opponents.

The internet offers both opportunities and challenges to the United States as it creates and occupies a new global commons. Its representatives will need to conduct a sustained strategic campaign to operate in this new environment and minimize its use as a distributed sanctuary and communications tool for evolving insurgent and terrorist organizations. In its pursuit of insurgents and terrorists, it needs to make the internet a priority in its strategic endeavors. As General of the Army Douglas MacArthur once suggested:

We must hold our minds alert and receptive to the application of unglimped methods and weapons. The next war will be won in the future, not in the past. We must go on, or we will go under.³⁵

The opportunities and challenges the internet contains are great, and Americans ignore them at their own peril.

ENDNOTES - CHAPTER 11

1. The National Security Strategy of the United States of America dated September 2002 is the baseline federal document outlining the strategic security posture for the United States. All other U.S. Government and Department of Defense strategies flow from it.

2. George W. Bush, "National Security Strategy of the United States of America," Washington: The White House, September 2002, p. 17.

3. David Held and Anthony McGrew, eds., *The Global Transformation Reader*, 2nd Edition, Cambridge, MA, 2003, p. 3.

4. Thomas L. Friedman, *The Lexus and the Olive Tree*, New York, 1999, p. 93.

5. *Ibid.*, p. xv.

6. Wayne Lee, *To Rise from Earth*, New York, 2000, p. 12. The height at which space begins is 121.9 Kilometers; at this altitude, there is no atmospheric pressure on an object.

7. John Baylis, et al., *Strategy in the Contemporary World*, Oxford, 2002, p. 210.

8. Joint Chiefs of Staff, *The U.S. Department of Defense Dictionary of Military and Associated Terms*, New York, 1987, p. 317.

9. Thomas X. Hammes, *The Sling and the Stone*, St. Paul, MN, 2004, p. 38.

10. U.S. Congress, National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, New York, 2004, p. 170.

11. Angel M. Rabasa, et al., *The Muslim World After 9/11*, San Monica, CA, 2004, p. 45.

12. Brett F. Woods, *The Art and Science of Money Laundering*, Boulder, CO, 1998, pp. 178-179.

13. Hammes, p. 40.

14. Rabasa, p. 44.

15. *Ibid.*, p. 40.

16. J. F. Rischard, *High Noon*, New York, 2002, p. 29.

17. Friedman, p. 325.

18. Joint Chiefs of Staff, "Joint Doctrine for Targeting," JP 3-60, p. vi, available from www.dtic.mil/doctrine/jel/new_pubs/jp3_60.pdf, Internet, accessed February 9, 2005.

19. *Ibid.*, p. C-2.

20. C. J. M. Drake, *Terrorists' Target Selection*, New York, 1998, pp. 175-182.
21. Norman Wade, *The Operations Smartbook-FM 3.0 Operations*, Florida, 2002, p. 1-50 to 1-51.
22. Rischard, p. 20.
23. JP 3-60, p. C-3.
24. Bruce Berkowitz, *The New Face of War*, New York, 2003, p. 10.
25. *Ibid.*, p. 11.
26. Walter Laqueur, ed., *"Voices of Terror" Manifestos, Writings, and Manuals of Al Qaeda, Hamas, and other Terrorists from Around the World and Throughout the Ages*, New York, 2004, pp. 405-406. The stated second source of information for providing the other 20 percent of the needed information on a target is classic human intelligence (HUMINT) collection or espionage.
27. Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York, 2003, pp. 88-89.
28. Bush, "National Security Strategy of the United States of America," p. 1.
29. Zalmay M. Khalilzad and John P. White, eds., *The Changing Role of Information in Warfare*, Santa Monica, CA, 1999, pp. 253-281.
30. JP 3-60, p. III-4.
31. George W. Bush, "National Security Strategy of the United States of America," p. 21.
32. Friedman, p. 322.
33. Peter G. Tsouras, ed., *The Greenhill Dictionary of Military Quotations*, London, 2000, p. 137.
34. George W. Bush, "The National Strategy to Secure Cyberspace of the United States of America," Washington, DC: The White House, February 2008, p. xviii.
35. Peter G. Tsouras, *Warriors' Words: A Quotation Book*, London, 1992, p. 222.