USAWC STRATEGY RESEARCH PROJECT

CYBER WARFARE/CYBER TERRORISM

by

Lieutenant Colonel Timothy F. O'Hara
United States Army

Ms. Cindy Ayers
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

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 **03 MAY 2004**	2. REPORT TYPE	3. DATES COVERED **-**
4. TITLE AND SUBTITLE **Cyber Warfare/Cyber Terrorism**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Timothy O'Hara**		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**		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 **See attached file.**		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**34**	

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

ABSTRACT

AUTHOR: Timothy F. O'Hara

TITLE: Cyber Warfare / Cyber Terrorism

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 34 CLASSIFICATION: Unclassified

This paper is divided into three parts. The first part of this paper will provide an overview of cyber warfare as an element of information warfare. It continues with the general background of the current strategic environment we are operating in. It will review why information warfare has become such an attractive alternative form of conflict and it will review the traditional principles of warfare and why they may or may not apply any longer to cyber warfare. It will also propose new principles of warfare that might be needed to conduct cyber warfare. This section will then conclude with a review of offensive and defensive cyber warfare concepts.

The second part gives a general overview of cyber terrorism. It will offer the reader a definition of cyber terrorism and cyber terrorism support. This section will examine three possible levels of cyber terrorist attacks. It will conclude with an analysis of the factors that may or may not encourage terrorists to engage in cyber terrorist operations.

The third and final section of this paper will attempt to answer the question "Is cyber terrorism a legitimate threat?" It will examine other factors that should be considered when evaluating cyber terrorism as a potential threat.

TABLE OF CONTENTS

ABSTRACT.....III

LIST OF ILLUSTRATIONS VII

LIST OF TABLES IX

CYBER WARFARE/CYBER TERRORISM 1

ENDNOTES 21

BIBLIOGRAPHY 23

LIST OF ILLUSTRATIONS

FIGURE 1.....6

FIGURE 2.....10

FIGURE 4.....12

FIGURE 5.....13

FIGURE 6.....16

LIST OF TABLES

TABLE 1. 6

TABLE 2. 7

TABLE 3. 11

TABLE 4. 14

CYBER WARFARE/CYBER TERRORISM

> "Our foes have extended the fields of battle – from physical space to cyberspace."
>
> —President Clinton, 22 May 1998

The way we conduct our conflicts is a reflection of our society. This is not a unique observation. In their book *War and Antiwar*, Heidi and Alvin Toffler observed that the way warfare is conducted is a reflection of the historical period. They divided human history and their corresponding conflicts into three waves. The first wave was the Agrarian Wave. The second wave was the Industrial Wave and the third wave, the current phase, is the Information Wave.

In their book, the Tofflers argued that Agrarian Wave warfare was conducted mainly for the control of local resources and reflected the agrarian nature of the era. Warriors were either members of the parties in direct control of the disputed resources or were conscripted tenants of feudal estates. Maintaining large standing armies was generally not feasible due to resource constraints. Those who manned the armies were also needed to tend the land. The groups who were able to maintain large standing armies and retain their agricultural base ensured their military dominance over others.

The Industrial Wave was the era of mass production. Warfare was conducted on a mass production basis. Large standing armies were produced and maintained. Entire societies were engaged in warfare with other societies. The entire productive effort of a society was required to support the war. Consequently, societies as a whole had a much greater investment in the winning and losing of such conflicts. Conflicts were no longer limited to combatant personnel. Non-combatants were now equally at risk.

The Tofflers concluded that we are currently in the Information Wave of warfare. Mass production has been replaced with unit production and specialization. Specialization encourages balkanization of people and resources. Mass production has been replaced with information specialization. Our dependency on technology, information, and interconnectivity to accomplish information specialization is growing at an exponential rate. Correspondingly, the way we conduct our military conflicts has changed from a mass production approach to an informational approach requiring specialization.

This paper is divided into three parts. The first part will provide an overview of cyber warfare as an element of information warfare. It continues with the general background of the current strategic environment we are operating in. It will review why information warfare has become such an attractive alternative form of conflict and it will review the traditional principles

of warfare and why they may or may not apply to cyber warfare. It will also propose new principles of warfare that might be needed to conduct cyber warfare. This section will then conclude with a review of offensive and defensive cyber warfare concepts.

The second part gives a general overview of cyber terrorism. It will offer the reader a definition of cyber terrorism and cyber terrorism support. This section will examine three possible levels of cyber terrorist attacks. It will conclude with an analysis of the factors that may or may not encourage terrorists to engage in cyber terrorist operations.

The third and final section of this paper will attempt to answer the question "Is cyber terrorism a legitimate threat?" It will examine other factors that should be considered when evaluating cyber terrorism as a potential threat.

In an effort to limit the scope of this paper the author has made some basic assumptions. First, the paper does not differentiate between the cyber activities conducted by hackers, activist groups, terrorist organizations, or nation-states. The logic behind this assumption is simple. Each group may have different motivations and target sets, but the technical tools they will use to launch their cyber warfare operations are the same. Second, it is assumed that our collective cyber security is only as good as the weakest link in the cyber chain. If in fact we are living in a truly "networked" environment then a minimal level of cyber security must be maintained to ensure the safety of all. Next, this paper was written with the typical commercial information system in mind. Specialized military information systems or information systems that are "air-gapped," are the exception and are outside the scope of this paper. Finally, cyber threats conducted by "insiders" are not addressed. The threats that insider attacks pose to cyber systems are significant, but the issues raised by this problem exceed the scope of this paper.

"May you live in interesting times."

—Ancient Chinese Proverb / Curse

The United States currently faces an increasingly hostile and unfriendly world. The collapse of the former Soviet Union has created a uni-polar environment with fewer constraints. Increasingly we are seeing the balkanization of areas, which were previously united. Regional nationalism, culturisms and other area specific issues, which were once covered over, have now surfaced. The increased interest in religious fundamentalism and intolerance is fueling already sensitive regional antagonisms. None of these regions shared the recent period of global economic prosperity. The gap between the countries who did prosper economically and those

who did not continues to grow. Flashpoints along the world's cultural fault lines have increased and many are ready to explode. Each represents a potential threat to the interest and security of the United States. Our involvement in these flashpoints makes us a lightning rod for criticism and direct action by those who are not satisfied with United States policy.

In many ways the current world situation is a result of United States successes in world affairs. The United States is a victim of a Cold War / Gulf War paradox--as the world's only remaining superpower, the harder we work to defeat our primary enemies the more open we become to attack by other lesser enemies. Our recent military victories, especially after our efforts in the Gulf War, clearly prove to those who would wish us harm that we cannot be successfully attacked in the traditional political, economic, and military manner. Our adversaries realize this and consequently understand that the only opportunity to achieve their political, social, or economic objectives lay in the ability to attack us through warfare by other means (WBOM)

WBOM can be expressed in two forms. The first form is the kinetic attack. A force-on-force engagement would best represent a traditional kinetic attack. When forces are asymmetric, the traditional form is not always feasible; therefore, suicide bombers might be used. A strategically planned suicide attack can have an impact well beyond its immediate operational results. The United States learned this costly lesson in Beirut when the Marine barracks were destroyed and again on September 11, 2001.

The second form of WBOM is the non-kinetic attack. This type of attack is not aimed at physical destruction but is designed to impact the adversary's will to fight and decision making process. Traditionally, this form of warfare is the propaganda or disinformation campaign. The historic successes or failures of these types of campaigns have been hotly debated. Cyber warfare is now a primary tool in the information warfare arsenal to achieve non-kinetic attacks. It should be noted that non-kinetic attacks could have kinetic results. For example, a non-kinetic attack on the decision making process of an adversary could result in the adversary making decisions that have effects in the physical world.

The value of non-kinetic attacks on an adversary is not a new concept, and its importance has been repeatedly emphasized throughout the study of warfare. Sun Tzu, in *The Art of Strategy,* realized the value in manipulating the decision making process of the enemy commander and recommended in battle: "use the normal force (direct approach) to engage; use the extraordinary (indirect approach) to win."[1] General Von Clausewitz in his tome *On War* realized the value of non-kinetic attacks as a means to increase the "fog of war." In our own century, Sir Basil Liddell Hart in his epic book *Thoughts on War* realized the real target in war is

the “mind of the enemy commander, not the bodies of his troops.” Strategic non-kinetic attacks are directly aimed at the hearts, minds, and the decision making process of the adversary. [2]

Cyber warfare is a very attractive means to accomplish non-kinetic warfare. It has many features that our adversaries would find attractive. Some of the most notable features are[3]:

- Low Entry Cost: For the price of a computer and connection to the Internet anyone can conduct cyber warfare operations. A variety of cyber warfare tools are openly available on a multitude of Internet sites worldwide. Consequently, the potential number of organizations capable of conducting cyber warfare against the United States is incalculable.
- Blurred Traditional Boundaries: Cyber warfare creates its own fog of war. Given the infinite number of potential threat organizations, the number of different cyber attack tools and the interconnectivity of the World Wide Web, it becomes increasingly difficult to determine between foreign and domestic sources of cyber warfare. This creates a cyber response dilemma. If you don’t know who is attacking you, who responds and how do you respond to the incident? Within the United States government, responses to cyber incidents are conducted by different agencies that are maintained as separate entities for legal reasons. The use of third parties by adversaries to conduct cyber warfare attacks can further complicate this issue.
- Expanded Role for Perception Management: Our adversaries now have the ability to effortlessly manipulate public perception by digitally manufacturing information or altering multimedia files. The cyber world never sleeps—it is available 24 hours a day. Perception management requires an equal amount of counter-perception management. This effort consumes valuable resources. Counter-perception management may detract from the original mission or may cause the mission to be canceled outright if the efforts are not successful. American participation in Somalia Operations from 1992-1994 was a case in point. The Clinton administration’s efforts were doomed when it could not counteract the negative domestic perceptions caused by photos showing a dead American service member being dragged through the city streets of Mogadishu.
- Lack of Strategic Intelligence: Traditional intelligence gathering methods and subsequent analytic techniques are outdated. Current intelligence and law enforcement organizations are not prepared for cyber warfare intelligence gathering. The blurring of traditional boundaries is a factor in this issue. Who, legally, collects what intelligence on whom? Adversaries will operate on Internet time and are able to

stand up and take down cyber attack centers faster than our ability to identify and evaluate their intentions.

- Difficulty of Tactical Warning and Attack Assessment: As a result of the ease and availability of cyber warfare tools and the fact that anyone can potentially launch a cyber attack, there is little to differentiate the “thrill-seeker” attack from the nation-state attack. Consequently, the United States may not know when an attack is underway, how the attack is being conducted, or by whom. The anonymous nature of cyberspace can be pierced over time but the initial cyber assault favors the attacker.
- Difficulty in Building and Sustaining Coalitions: Coalition warfare is the United State’s warfare method of choice. However, collective network security is only as good as the weakest link. Less technically advanced coalition partners may not be up to current technical standards and may represent a potential backdoor into United States information systems. Upgrading the security posture and ensuring that our coalition members are not potential targets will require a significant investment of our resources.
- Vulnerability of US Homeland: Current studies indicate that the United States will be increasingly dependant on complex, interconnected, and networked information systems. Consequently, our vulnerability to cyber warfare operations will increase over time, thus providing our adversaries with a target rich environment.

The cost of conducting a traditional kinetic attack is too high for our adversaries to sustain. Traditional kinetic attacks are limited in scope and only affect the military, physical, and economic planes of our society. In order to achieve their objectives, our adversaries must turn to WBOM. Non-kinetic attacks, as expressed in cyber warfare, offer adversaries greater opportunities to directly impact the United States homeland on the political and social as well as the military, physical and economic planes of our society.

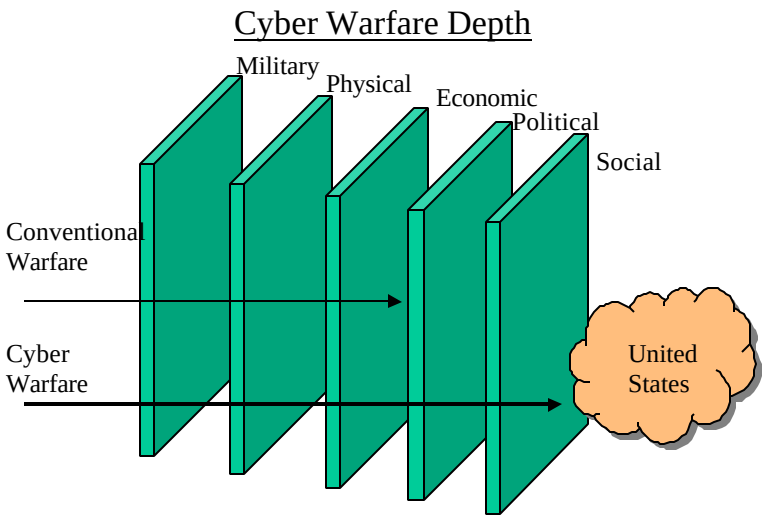

FIGURE 1.[4]

Cyber warfare does not follow the generally accepted principles of warfare in the traditional sense. Those principles of warfare were based on an Industrial Wave method of waging warfare. While some are applicable to the conduct of cyber warfare, others are not. The following chart summarizes the generally accepted principles of warfare in a cyber war context[5]:

Principle	**Relevance**
Mass	Old: Bringing together all available kinetic forces to overwhelm the enemy at one place and one time. New: Bring together all available cyber forces to overwhelm the enemy at a specific cyber space location and time. Mass is not restricted to the use of friendly cyber forces. For example a denial of service attack may use multiple friend or foe computers to attack one computer at a specific time. Cyberspace provides the ability to swarm resources.
Objective	Remains the same. Specific targeting of the adversary's key center of gravity.

Offense	Old: Maintain offensive operations to preserve the freedom to dictate the operational tempo of the campaign. New: Not as relevant. Adversarial cyber war operations can occur anytime, anyplace. No longer limited to inherently military targets.
Surprise	Remains the same: Pick the time and place for cyber warfare operations against our adversaries where they least expect it or at times when their security level is at a minimum
Economy of Force	Remains the same: Cyber warfare is the ultimate application of the economy of force principle. One attacker has the ability to tie up the adversary's resources well out of proportion to the attacker's size. Unwitting third parties may be pressed into service.
Maneuver	Remains the same: Use of the Internet allows adversaries to switch their point of attack quickly and efficiently. Ability to maneuver in cyberspace is greater than physical space.
Unity of Command	Old: Maintain unity of command to maintain unity of forces in the drive to obtain a single objective. New: Maintain general commonality of effort. Internet allows a confederation approach of different groups to achieve a common set of goals.
Security	Remains the same. Added importance as unknown and infinite number of adversaries can now strike from any direction at any time.
Simplicity	Remains the same. Cyber war operations are technically challenging. However, this does not mean the overall mission objective needs to be challenging. Those cyber operations that are the simplest in scope have the best chance of success. For example, a recent successful cyber attack targeted the common network printer buffer protocol.

TABLE 1.

Cyber space is a unique environment with its own set of physical laws. The use of cyber warfare as a component of information operations requires new principles of warfare to be considered. Future principles of cyber warfare should include the following[6]:

Physical Effects	Cyber warfare is irrelevant unless it has an effect in the physical world. Media pundits write about using cyber warfare to open floodgates or cause power grids to fail. This is beyond the ability of current cyberspace operations. A more practical example of this principle is to change something in cyberspace that will manipulate the judgment and actions of adversary decision makers in the physical world.
Visibility	Cyber space is an artificial environment. Although it is often difficult, offensive and defensive cyber operations can be tracked. Cyber warfare operations are not stealth operations. Properly set cyber defenses will, eventually, detect cyber-based operations.

Reliability	Because cyberspace is an artificial environment it is not consistent or reliable. Hardware and software configurations vary widely and do not always work as expected. Local technical conditions can effect cyber operations in unexpected ways and have unintended consequences. Cyber war operations may not accomplish their objectives.
Duality	Cyber tools can be of use in offensive and defensive operations by either friend or foe. For example, a packet scanner can be used to detect an adversary's vulnerabilities as well as to identify and correct internal weaknesses of friendly forces.
Equipment Defense	Both the cyber defender and attacker control only a very small portion of the cyberspace. Whoever can control the part of cyberspace that their opponent uses, can control the opponent. Controlling an opponent's cyberspace equates to dominating the opponent's cyber equipment either directly or indirectly.
Physical Constraints	Physical constraints limit cyberspace operations. Hardware, software, and information systems must operate within their technical parameters. This creates artificial boundaries, which will limit the possible scope of cyber operations.

TABLE 2.

> "The real target in war is the mind of the enemy commander, not the bodies of his troops."
>
> —Captain Sir Basil Liddell Hart
> Thoughts on war

Offensive cyber warfare can be conducted across the entire range of military and non-military operations to achieve national objectives. The employment of cyber warfare to affect an adversary's information capabilities can be a tremendous advantage to the United States in times of crisis or conflict. The decision to utilize offensive cyber warfare operations should be made only after coordination within the highest levels of our government. Improperly coordinated or approved offensive cyber warfare operations have the potential to be self-disruptive to the attacker.

Offensive cyber warfare may be the main effort or the supporting effort in an information warfare operation. In either case, the principle objective of offensive cyber warfare is to target the adversary's human decision-making process.[7] Being consistent with our basic principles, offensive cyber operations should achieve a physical world result. Clearly articulated offensive cyber war objectives should support our overall national objectives during the entire peace-

crisis-conflict-peace continuum. Use of cyber warfare as a tool in achieving our national objectives is no different from using a non-cyberspace warfare tool. The selection of offensive cyber war objectives should be appropriate to the situation and consistent with applicable domestic and international laws. [8]

Offensive cyber war operations fall into one of three categories: destruction, disruption, or disinformation.[9] Cyber operations that result in the destruction of physical assets are currently not a reality. To date, not a single incident of physical destruction resulting from a computer virus or another form of cyber type attack has been reported. It is possible that this capability might be developed in the future. However, it is unlikely that any but the most technologically advanced adversaries will be able to develop this capability. Research and development efforts should be continued to further explore this option and ensure that it remains only a possibility.

Disruption is the most likely and common form of offensive cyber warfare. This type of operation can best be exemplified by web page defacements, the releasing of computer viruses, worms, and other software attacks aimed at damaging critical data within information processing systems. The level of sophistication needed to unleash this type of attack is very low. Tools are available on the Internet that anyone can download and launch. The desired result of this type of operation is to deny (at least temporarily) the adversary the use of their information systems and cause them to expend valuable resources on system restoration. Disruption operations should be used sparingly, however. Once released, disruptive attacks are difficult to control, and may affect the attacker as much as the defender.

Disinformation involves the deliberate manipulation of information with the intent of placing the adversary in the worst public opinion position possible. The objective of this option is to create a hostile climate to the adversary's policy position so that public opinion will cause them to modify their position. Disinformation differs from the other two forms of offensive operations in the sense that it targets not only the adversary, but also those who might assist the adversary. Disinformation is the least intrusive form of the three types of offensive cyber war operations, as it does not depend on interacting with the adversary's information system. One major disadvantage of this type of operation is that the attack execution must be managed in fine detail. Exposing the source of disinformation may result in a backlash against the perpetrator and a consolidation of support for the adversary.

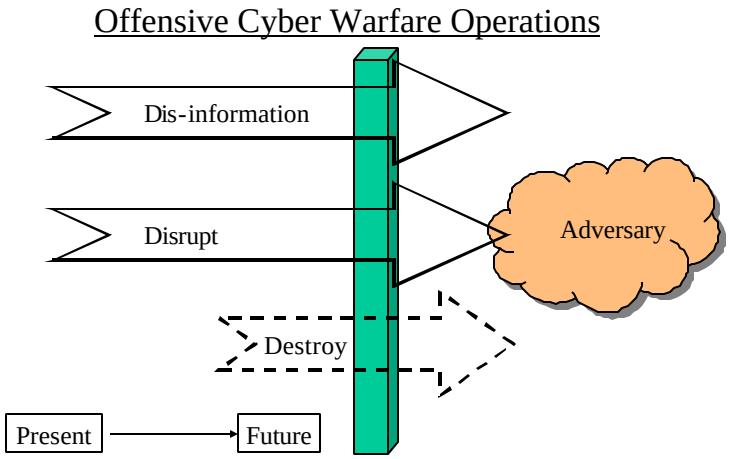

FIGURE 2.

> "Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."
>
> —Frederick the Great, 1749

Defensive Cyber warfare is designed to operate across the entire range of military and non-military operations to achieve national objectives. Cyber systems serve as enablers and enhance our national capabilities. Maintaining the freedom to use our cyber systems is a key national objective. The primary intent of defensive cyber warfare is to ensure the necessary protection and defense of our key critical infrastructure. Unlike offensive operations, defensive

operations do not require the same level of close coordination and high-level approval. Defensive cyber operations should be conducted widely and down to the lowest level possible.

There are four key goals in cyber defense. The first is to establish a protective cyber environment. Maintaining a protective environment will allow us to retain the freedom to use our systems when and where we need them. The second is attack detection. As previously stated one of the key reasons why cyber warfare has become an attractive form of warfare is because it can create its own "fog of war." Systems, which are not configured correctly or unsupervised, may not even realize that they are under attack. Third, systems that have been compromised need to be restored quickly and efficiently. Often the effects of being compromised can be mitigated if a system can be restored quickly. The fourth and final goal is attack response. Defensive and offensive cyber operations are mutually supporting. Good defensive operations will point in the direction of the attacker, which then allows offensive operations to target them for retaliation.[10]

Defensive operations will fall into one of five categories. They are designed to ensure confidentiality, integrity, availability, non-repudiation, and authentication of friendly systems. The following chart summarizes the key features of each of these categories [11]:

Category	**Summary**
Confidentiality	Actions designed to ensure information is not disclosed to unauthorized personnel.
Integrity	Actions designed to ensure the consistency of information by preventing unauthorized creation, alteration, or destruction of data.
Availability	Actions designed to ensure that legitimate users are not unduly denied access to resources, including information, computing, and communications resources.
Non-repudiation	Actions designed to ensure that a party to a communication cannot later falsely claim that the communication did not take place.
Authentication	Actions designed to ensure the identity of the principals of a transaction.

TABLE 3.

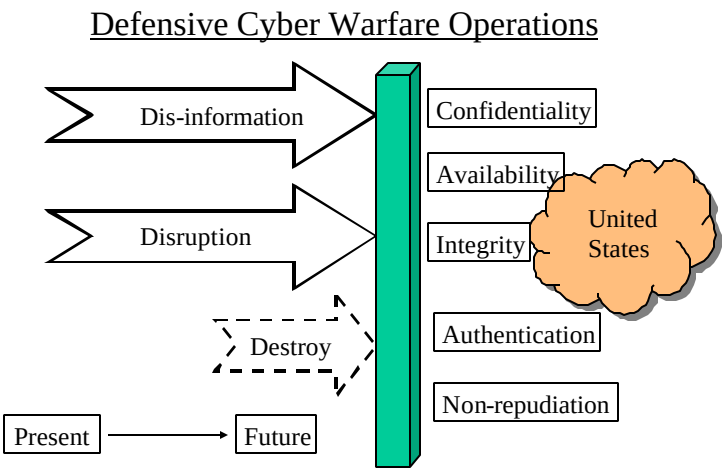

FIGURE 4.

Offensive and defensive cyber operations are key elements of information warfare. They are available to support the entire spectrum of national security affairs. In times of peace, they work with other elements of national power to prevent crisis and conflict. In time of crisis, they can help shape the situation to our advantage and help avoid potential escalation. In times of conflict they can be used to help win the fight as a kinetic force multiplier and then assist in the transition to peacetime operations.

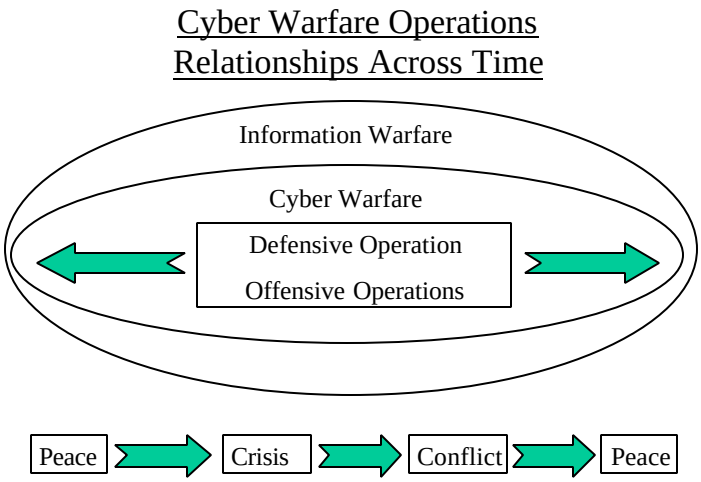

FIGURE 5[12].

"Terrorism is, among other things, a weapon used by the weak against the strong."

—Ian O. Lesser
Countering the new terrorism: Implications for Strategy

The academic and political debate regarding cyber terrorism is intense. The study of cyber terrorism suffers from many of the same issues as the study of traditional terrorism. First, there is no generally accepted definition for cyber terrorism. For the purpose of this paper, cyber terrorism is defined as:

- The unlawful destruction, disruption, or disinformation of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological. [13]

The focus of this definition differs from a more traditional definition of terrorism in the sense that it centers on the manipulation of digital property. It has not been proven that cyber terrorism can have any direct effect on physical property or people. Cyber terrorism, by its nature, exists only in cyberspace and thus its direct effects are limited to that domain. This is not to imply, however, that cyber terrorism does not have an indirect effect in the physical world. The previous portion of this paper clearly indicated that cyber warfare, and thus cyber terrorism, could have non-kinetic effects.

Cyber warfare has the potential to act as a force multiplier. The cyber terrorist can also take full advantage of this concept. Consequently, a second definition is offered regarding the terrorist's use of cyberspace in support of terrorist operations. Cyber terror support is defined as:

- The unlawful use of information systems by a terrorist or terrorists that is not intended, on its own, to have coercive effects on a target audience. Cyber terrorism supports, augments, or enhances other terrorist actions.[14]

The primary goal of a cyber terrorist may not be to disrupt, destroy, or "dis-inform" cyberspace. The primary goal might be to use cyberspace to "augment or enhance" some other physical threat or act of terrorism.[15] These activities may include acts of intelligence collection, communications, logistical coordination, and perception management (i.e. "spin control").

Not all cyber attacks are "created equal."[16] The scope and degree of destruction, disruption, or disinformation of a cyber attack is clearly indicative of the cyber terrorist's capabilities and objectives. Technical analysis of potential cyber attacks has allowed categorization into three broad categories. The following chart summarizes these possible categories[17]:

Attack	**Target**	**Effect Control**	**Utility**	**Level of expertise needed**
Simple Unstructured	Single System or Network	Unfocused	Disruption	Low
Advanced Structured	Multiple Systems of Networks	Basic	Disruption Destruction of Data	Medium
Complex Coordinated	Multiple Networks	Sophisticated	Disruption Destruction of Systems	Very High

TABLE 4.

Simple Unstructured attacks are defined as[18]:

- The capability to conduct basic level attacks against individual systems using tools created by someone else.

The primary goal of this attack is to disrupt target operations. Typically, the organization or individual that launches this level of attack has little target analysis capabilities, command and control, or higher education. They are the most common and basic form of attacks on the Internet today. The terrorist downloads available hacker tools and launches them against the intended target. The attack is limited in duration and consequence. Recovery from this type of attack requires minimal effort and may be negated in its entirety if adequate cyber defenses are in place.[19]

Advanced Structured attacks are defined as[20]:

- The capability to conduct more sophisticated attacks against multiple systems or networks and to modify or create basic hacking tools. The organization possesses an elementary target analysis capability and command and control structure for sequential attacks from a single location. The organization or individual has the ability to learn and assimilate new technologies independently and they can train others to use these technologies.

The primary goal of this type of attack is to disrupt and destroy target operations. Organizations or individuals that are capable of this level of attack employ a much higher level of cyber sophistication and education than the Simple Unstructured cyber terrorist. The use of an Advanced Structured attack also indicates an ability to conduct reconnaissance in order to target specific vulnerabilities and achieve specific target objectives. At this level the attacker is not just downloading free attack software but also modifying the programming of attack tools themselves. The capability to launch this level of attack is an indicator that the cyber terrorist is part of a much larger and well-resourced organization that may have non-cyber based terrorism objectives. Efforts to recover from this level of cyber attack will require significant time and resources. Efforts to defend against this level of attack will require a moderate level of commitment to employing cyber defense technologies and trained personnel.[21]

The final level of cyber attack is the Complex Coordinated Attack. This attack is defined as[22]:

- The capability to coordinate cyber attacks causing mass disruption or data destruction. The organization—no longer just an individual—capable of this level of attack has a very high ability to analyze target vulnerabilities, penetrate integrated heterogeneous defenses and create unique attack tools. The organization has a strong command and control structure able to employ multiple and simultaneous

attacks from different locations. It is a very high knowledge-centric organization, consisting of individuals capable of creating their own cyber warfare tools, doctrine, and organizations.

An organization capable of this level of attack is the ultimate cyber warrior group. An operational example would be all-out cyber warfare on the national telephone network. Realistically, this type of cyber attack is well beyond the capabilities of most, if not all, currently typical terrorist groups. It is not, however, beyond the capability of a select group of nation-states who might use cyber terrorism as WBOM. Cyber attacks conducted at this level are extremely technical and sophisticated, but the probability of occurrence at this point in time is low due to the high level of expertise and the resources needed to launch them. If successfully launched, the result could be devastating and would be felt on a national level. Recovery efforts would be very resource and time intensive.[23]

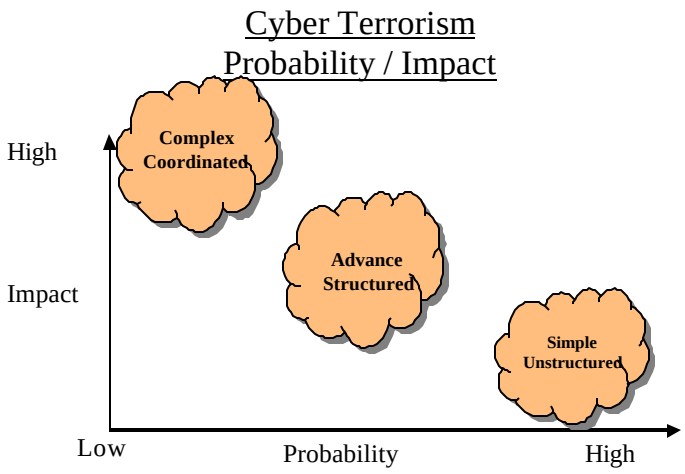

FIGURE 6.[24]

Having identified potential cyber terrorist attacks, the question now is, are terrorists motivated to pursue cyber terrorism as a method of operation? Cyber terrorism offers the terrorist the opportunity for remote access to global targets. With the increased level of global dependence on computer technology, cyber terrorism offers the terrorist new forms of asymmetric warfare. Ironically, the lack of a worldwide consensus on what constitutes a cyber

terrorist act, offers the terrorist a level of legal protection that is not available for a physically based attack. Additionally, depending on the attack methodology, cyber terrorism is a low cost operation. In short, many of the incentives to conduct cyber terror attacks are very similar to, if not the same, reasons that have made cyber operations an attractive form of Information Warfare.[25]

Equally, there are many disadvantages for the common terrorist to engage in cyber terrorism. Terrorist groups, like any other organization, operate with constrained resources. While the cost of cyber operations is low, the attacks may not achieve the organization's desired strategic objective. This is especially true of terrorist groups that want to cause physical death and destruction. Additionally, the use of cyberspace is not completely anonymous and counter terrorism forces are well equipped to track down those who launch cyber attacks. Consequently, cyber terrorists will have to decide if the possibility of compromising their base of operations is worth the result of their cyber attack. Finally, cyberspace is an uncertain realm and the results of a cyber attack are not guaranteed. Terrorists may not want to commit resources to an unproven method.[26]

The decision to use or not use cyber terrorism as a method of operation also depends on the group. Different terrorist groups have different goals. Cyber terrorism may not be in accordance with the group's objectives. Religiously based terrorist groups have not demonstrated an overwhelming desire to use cyber terrorism possibly because it does not result in death, destruction, or have a high media payoff. In contrast, groups intent on disrupting the commercial operations of large business corporations are conducting cyber terrorist operations.[27] The location of the group's base of operation is also a factor. Cyber terrorism requires access to technological resources. A group based in the jungles of Peru, with limited Internet access, is less likely to engage in cyber terrorism than a group located in the Federal Republic of Germany which has unlimited access to the Internet.

In the end, however, the level of a group's technical abilities may ultimately decide if a terrorist organization will conduct cyber terrorism operations. Technical skills are not a critical discriminator for the lower, less sophisticated level of attacks. They are very critical if the group wants to accomplish a medium level, Complex Coordinated, or a high level, Advanced Structure, attack. A terrorist group could have the desire, but find itself without the skills necessary to conduct cyber terrorist operations precisely when they are positioned in a location that will enable them to launch an attack.[28]

“Threat analysts warn us of our vulnerabilities yet overlook our strengths.”

—Ralph Peters
Fighting for the Future

In concluding this discussion on cyber terrorism it is important to consider some other issues that have not been fully explored and answer the ultimate question--is cyber terrorism a legitimate threat? Is the threat at the level that we may suffer a “Digital Pearl Harbor?” Are there no other mitigating factors?

First, consider that cyber terrorists must deal with the difficulty of attacking constantly moving targets. Cyber defenses are not static. One of the benefits of inflaming public passions about the threat of cyber terrorism is that the public, as a whole, is much more aware of the threat and the need to take preventive counter measures. Hardware, software, and personnel are being upgraded and trained to ensure cyber defensive measures are a part of all automation operations. The Cyber Corps program at the University of Tulsa is a living testament to the increased importance being placed on national cyber security. The dynamic nature of cyber security is, in itself, adding to the ability to defeat cyber terrorist operations.

Second, the increased use of automation systems has resulted in the wide spread reduction in administrative personnel. Reduction does not equate to elimination. Many cyber systems--because of security, liability, or mission criticality reasons--retain personnel in the system to supervise operations and provide over watch functionality. The person-in-the middle (PIM) is a key factor in helping to defeat cyber terrorist operations. Not only must the cyber terrorist get by cyber defense systems but they must also overcome the final human defender. In many ways it is the final PIM that makes cyber terrorism operations so unreliable.

Third, cyber terrorism is a technical operation. While it is important to analyze the human aspect of the threat, it is more important to focus on the technical threat cyber terrorism poses. Recent intelligence failures clearly show that the number of different groups that pose a threat to the security of the United States is almost limitless. Our ability to identify and target these different groups is resource limited. In contrast, cyber terrorism as a technical operation has a finite set of attack points. Defend these cyber defense points and you will mitigate or defeat the ability of the cyber terrorist to conduct these types of technical attacks.

In conclusion, cyber terrorism is not fictional concept. Cyber terrorism is a real and a legitimate threat. Cyber attacks at the low to medium level do occur on a regular basis. However, study clearly indicates that cyber terrorism, as a threat, is not currently and has not been at the level the media pundits would have us believe. A “digital Pearl Harbor” is certainly conceivable, but it is probably unlikely, and the threat diminishes as the level of awareness

increases. Correspondingly, the threat of a cyber attack resulting in physical damage is equally unlikely. What is more likely to occur in the future is a steady increase in the number of cyber attacks that we are currently experiencing. These attacks are designed primarily to disrupt digital data and “dis-inform” the public. It is also more likely that the future will see a steady increase in the use of cyberspace to support general terrorist operations. For the same reasons that private businesses and governments derive value added from cyber operations, so will terrorists.

In spite of the events of September 11th we live in an optimistic time. The terrorist group that attacked us on our home soil is on the run. While still dangerous, their over-all effectiveness has most likely been reduced. Although cyberspace is not a risk-free environment, the benefits of private, business, and governmental usage of cyberspace clearly outweigh the risks. The freedom of cyberspace can be maintained, as long as domestic cyber security measures are properly structured so as to minimize damage resulting from intentional cyber attacks.

WORD COUNT= 5997

ENDNOTES

[1] *Joint Publication 3-13 Joint Doctrine for Information Operations*. (Washington, D.C.: Department of Defense, 1998), I-1.

[2] Raymond C. Parks, *Principles of Cyber-Warfare*. (Proceedings of the 2001 IEEE workshop on Information and Security), 122.

[3] Rodger C. Molander, *Strategic Information Warfare. A new face of war*. (Santa Monica, CA: Rand Corporation, 1996), XIV.

[4] Ibid., 12.

[5] Parks, 123.

[6] Ibid.,123.

[7] *Joint Publication 3-13,* II-1

[8] *Ibid.,* I-4 and Chapter II.

[9] Ibid., II-11

[10] Ibid., III-1.

[11] Ibid., III-3.

[12] Ibid., I-4.

[13] Major Bill Nelson, *Cyberterror, Prospects and Implications*. (Monterey, CA: Center for the Study of Terrorism and Irregular Warfare. Naval Post Graduate School, 1999), 9.

[14] Ibid., 10.

[15] Ibid., 10.

[16] Ibid., 13.

[17] Ibid., 15.

[18] Ibid., 14

[19] Ibid., 14.

[20] Ibid., 16.

[21] Ibid., 16.

[22] Ibid., 16.

[23] Ibid., 16.

[24] Ibid., 73.

[25] Ibid., Chapter III.

[26] Ibid., Chapter III.

[27] Ibid., Chapter III.

[28] Ibid., Chapter V.

BIBLIOGRAPHY

Arquilla, John, and David Ronfield. *Networks and Netwars*. Santa Monica, CA: Rand Corporation, 2001.

Bush, George W..*The President's Commission on Critical Infrastructure Protection, The National Strategy to Secure Cyberspace* . Washington D.C.: The White House September 2002.

Cater, Ashton. *The Architecture of Government in the Face of Terrorism* . International Security, vol. 26.

Cordesman, Anthony. *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction* . New York, NY: Praeger Publishers Inc., 2002.

Cordesman, Anthony. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection* . New NY: Praeger Publications Inc., 2002.

Ford, Warwick, and Michael S. Baum. *Secure Electronic Commerce* . Upper Saddle River, NJ: Prentice-Hall Inc., 2001.

Garfinkel, Simson. *Web Security, Privacy, and Commerce*. Sebastopol, CA: O'Reilly & Associates, Inc., 2002

Green, Joshua, (2002). The Myth of Cyber Terrorism. http://www.washingtonmonthly.com/features/2000/0211.green.html. Accessed 1 December 2003.

Hart, Liddell. *The Strategy of Indirect Approach* . London, U.K.: Faber and Faber Limited., 1941.

Hart, Liddell. *Strategy*. New York, NY: Praeger Publishers Inc., 1954.

Hoffman, Bruce. *Inside Terrorism* . New York, NY: Columbia University Press, 1998.

Huntington, Samuel P.. *The clash of civilizations and the remaking of world order*. New York, NY: Simon & Schuster Inc., 1996.

Institute for Security Technology Studies. *Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Darmouth College, 2001.

Institute for Security Technology Studies. Combating Terrorism: *A Compendium of Recent Counterterrorism Recommendations from Authoritative Commissions and Subject Matter Experts*. Darmouth College, 2001.

Kusher, Harvey. *The Future of Terrorism: Violence in the new millennium* . London, U.K.: Sage Publications Inc., 1998.

Laquer, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford, U.K.,1999.

Lesser, Ian, Bruce Hoffman, John Arquilla and Michelle Zanini. *Countering the New Terrorism* . Santa Monica, CA: Rand Corporation,1994.

Molander, Rodger C., Andrew S. Riddile and Peter A. Wilson. *Strategic Information Warfare. A new face of war*. Santa Monica, CA: Rand Corporation, 1996.

Nelson, Bill, Major, Major Rodney Choi, Major Michael Iacobucci, Major Mark Mitchell, and Captain Greg Gagnon. *Cyberterror, Prospects and Implications*. Monterey, CA: Center for the Study of Terrorism and Irregular Warfare. Naval Post Graduate School. 1999.

Parks, Raymond C. and David P.Duggan. *Principles of Cyber-Warfare* . Proceedings of the 2001 IEEE workshop on Information and Security.

Pillar, Paul. *Terrorism and U.S. Foreign Policy*. Washington, DC: Brookings Institution Press. 2001.

Thomas, Douglas and Brian D. Loader. *Cybercrime, Law enforcement, security and surveillance in the information age* . New York, NY: Routledge Inc., 2000.

Sofaear, Abraham D. and , Seymour E. Goodman. *The Transnational dimension of cyber crime and terrorism* . Stanford, CA: Hoover Institution Press. 2001.

U.S. Joint Chief of Staff. *Joint Doctrine for Information Operations*. Joint Publication 3-13. Washington, D.C.: Joint Chief of Staff, 9 October 1998.

Wall, David S. *Crime and the Internet*. New York, NY:Routledge Inc., 2001.