The Department of Defense Must Combat Cyber Terrorism With Cyber Attacks

EWS Contemporary Issues Paper

Submitted by Captain P. A. Snyder
to
Major C. Lynn, CG 15

20 October 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
20 OCT 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Department of Defense Must Combat Cyber Terrorism With Cyber Attacks	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) **United States Marine Corps Command and Staff College,Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	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	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

The United States and its Allies are attacked daily. Critical infrastructure assets are exploited by terrorist actors from around the world. To prevent these attacks, new capabilities must be employed against terrorist organization members, their assets and their competencies. These capabilities must degrade their ability to wage both information and kinetic warfare against the US and its Allies. The Department of Defense (DoD) is unprepared to combat terrorism in cyberspace because it does not utilize offensive capabilities of cyber attack or active cyber defense against terrorist Command and Control (C2), training, political and physical capabilities.

Background

Until recently, the DoD did not acknowledge the requirement or existence of cyber attack capabilities. These cyber attack capabilities are intellectual and physical resources that can be used to destroy or limit technological assets used by adversaries. The biggest change to policy that allowed for cyber attacks occurred in October 2002 when the Joint Task Force-Computer Network Operations (JTF-CNO) was established under US Strategic Command.[1] This task force was charged with both Computer Network Defense and Computer Network Attack (CNA).[2] In

[1] Joint Task Force - Global Network Operations, http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html, accessed 14 December 2007

February of 2006, Joint doctrine was updated to state that computer network operations consist "of computer network attack, computer network defense, and related computer network exploitation enabling operations." [3] Establishing the Joint Task Force – Global Network Operations organization was the first step to implementing this new capability.

Before this doctrine was released, the information system policies of the military focused solely on passive defense. Each service organization, such as the Air Force Computer Emergency Response Team, was charged with monitoring and defending the network capabilities for their perspective service.[4] The process to secure the network that was implemented was to identify the threat, then block it from accessing our networks.

The limited passive defense actions these service organizations could execute effectively forced them to barricade themselves behind fortresses of security in order to protect themselves from threats. The JTF-CNO policies stopped short of allowing the DoD to retaliate or initiate any offensive actions

---

[2] US Army Training and Doctrine Command, DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism,* 15 August 2005, IV-4

[3] Department of Defense, Joint Publication 3-13, *Information Operations*, 13 February 2006, GL-6

[4] *Air Force Computer Emergency Response Team,* http://www.fas.org/irp/agency/aia/cyberspokesman/97aug/afcert.htm, accessed 14 December 2007

against those who attacked the DoD. Because of this restriction, the service organizations responsible for network security did not dedicate resources or training toward planning for or implementing cyber attack capabilities.

However, terrorists do have cyber attack capabilities and are working toward employing them to attack our assets from anywhere with an Internet connection. These hackers are trained by the terrorist organizations or they are freelance hackers who work with the terrorist organizations because they are motivated by religion, financial incentives, or their shared view of the US as a common enemy.[5] A February 2002 statement by al Qaeda stated:

> Despite the fact that the jihadi movements prefer at this time to resort to conventional military operations, jihad on the Internet from the American perspective is a serious option for the movements in the future for the following reasons:
> • First: Remote attacks on Internet networks are possible in complete anonymity.
> • Second: The needed equipment to conduct attacks on the Internet does not cost much.
> • Third: The attacks do not require extraordinary skill.
> • Fourth: The jihadi attacks on the Internet do not require large numbers [of people] to participate in them. [6]

[5] US Army Training and Doctrine Command, DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism,* 15 August 2005

[6] Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 36, quoting Abu 'Ubeid al-Qurashi, "The Nightmares of America", 13 February 2002. Quoted in US Army Training and Doctrine Command, DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism,* 15 August 2005

Terrorist use of cyberspace to attack US Command and Control

Terrorists use the Internet to coordinate and control both kinetic and information based attacks. "Thousands of encrypted messages that had been posted in a password-protected area of a website were found by federal officials on the computer of arrested al Qaeda terrorist Abu Zubaydah, who reportedly masterminded the September 11 attacks."[7] This trend continues today and has become more complex. Terrorists are using the Internet to transfer files that appear to be ordinary images, but actually have orders digitally embedded in them.[8]

These types of orders and messages for Command and Control (C2) purposes must be sought out and destroyed by US cyber attacks. Currently the DoD lacks the capability to disrupt these C2 messages through spoiling attacks against these transmissions in the form of e-mail, web sites, and the source and target computers. Failure to disrupt or destroy this

[7] Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, March 2004, http://www.usip.org/pubs/specialreports/sr116.html, accessed 14 December 2007

[8] Gina Kolata, *Veiled Messages of Terror May Lurk in Cyberspace*. New York Times, 30 October 2001, http://query.nytimes.com/gst/fullpage.html?res=9B01E3D91730F933A05753C1A9679C8B63&sec=&spon=&pagewanted=all, accessed 14 December 2007

capability enables terrorist organizations to plan and execute attacks freely from anywhere around the world.

Training

In addition to commanding forces, terrorists use the Internet as a way to perform on-line training for their recruits. A Google search of "bomb making instructions" yields 210,000 results including videos that show how to build a suicide vest.[9] Additionally, terrorist meet in on-line chat rooms and hold classes on subjects like how to use weapons or how to kidnap people.[10]

These activities must also be targeted by DoD cyber attacks. Sites that support training must be taken down to limit terrorist capabilities to train new recruits. This will reduce the effectiveness of their attacks and their ability to conduct worldwide training. The DoD is currently unable to disrupt this capability due to a lack of cyber attack competency.

Political

[9] Lisa Myers, *Web video teaches terrorists to make bomb vest*, 22 December 2004, http://www.msnbc.msn.com/id/6746756/, accessed 14 December 2007

[10] Louis Charbonneau, *Virtual Terrorist Training Camps Described*, 24 November 2007, http://www.pcworld.com/article/id,139897/article.html, accessed 14 December 2007

A less direct, but just as dangerous, threat is the terrorist organizations' use of the Internet to gain political support. They conduct fund raising operations and spread their message to people around the world. "One example of the use of the computer as a tool is by the Tamil Tiger terrorists, who were able to hack into Sheffield University in England in 1997, and use the university computer system to send their propaganda and to engage in fund raising."[11] Gabriel Weimann, a professor at the University of Haifa in Israel has completed numerous studies on terrorism. He stated that most organizations "will provide a history of the organization and its activities, a detailed review of its social and political background, accounts of its notable exploits, biographies of its leaders, founders, and heroes, information on its political and ideological aims, fierce criticism of its enemies, and up-to-date news."[12] This information is used to recruit both supporters and active participants who will join their cause.

The DoD is currently unable to employ a cyber attack capability to perform spoiling attacks to disrupt terrorist

[11] Yonah Alexander and Michael S. Swetnam, *Cyber Terrorism and Information Warfare*, (Transnational Publishers, 2001), http://www.terrorismcentral.com/Library/Teasers/vatis.html, accessed 14 December 2007

[12] Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, March 2004, http://www.usip.org/pubs/specialreports/sr116.html, accessed 14 December 2007

support. These spoiling attacks should target sites that enable terrorists to gain political support for their cause. In this particular area, extreme caution must be exercised. Many of these terrorist organizations are seen as legitimate political organization (i.e. Hamas) and if they are targeted, it may actually embolden supporters of the cause against the US. Because of this, the DoD must only employ this attacks against organizations that the US has identified as bone-fide terrorist organization and not state actors.

Physical/Direct Attack

Perhaps the most dangerous capability that terrorists may possess is the ability to launch cyber attacks against the US and its allies. These attacks are not just limited to attacks against computers but can destroy infrastructure, economic resources and security causing widespread disasters. In 2001 hackers reprogrammed Internet capable phones in Japan to always dial their version of 911, bringing emergency services to its knees.[13] Other attacks have broken into hospital databases and changed patient medication requests to lethal doses.[14]

[13] Institute For Security Technology Studies At Dartmouth College, *Cyber Warfare, An Analysis Of The Means And Motivations Of Selected Nation States*, December 2004, http://www.ists.dartmouth.edu/projects/archives/cyberwarfare.pdf , accessed on 14 December 2007

[14] Institute For Security Technology Studies At Dartmouth College, *Cyber Warfare, An Analysis Of The Means And Motivations*

These threats are the most serious. The DoD lacks active cyber defense capability to counterattack these actions. Passive defense capabilities clearly do not work and determined hackers are capable of getting around these barriers. To be effective at preventing destruction of our capabilities, the US must quickly identify when attacks are launched against its infrastructure and networks. They must then be poised to quickly counter attack and destroy the enemy capability to continue their attack.

Opposition

Opponents of CNA may cite that by destroying the terrorists' abilities to communicate, train and seek political support we are suppressing their basic right of free speech. While this may be true, these terrors are waging information warfare against the US. Americans therefore have the right to protect the nation against these threats by launching pre-emptive strikes against terrorists.

Other critics to the DoD use of cyber attack will conclude that the attacks will incite counter attacks against the US. This is highly possible, but if the DoD places emphasis on this action they will be able to better identify who the hackers are and what resources they are using to launch attacks. In the

---

Of Selected Nation States, December 2004, http://www.ists.dartmouth.edu/projects/archives/cyberwarfare.pdf , accessed on 14 December 2007

best case scenario, those with the skills and desire will attack and the DoD will be able to identify, attrite, and stop cyber-terrorism.

Finally, individuals against such action will argue that innocent servers and systems are often exploited and used to launch attacks. The owners of these systems (specifically known as proxy systems) often do not realize that they are even being used by terrorist organizations. In this case, launching a counter attack on the proxy system is actually a good thing in the long term. If system administrators have their systems shut down by the DoD because they have been used by terrorists, perhaps they will take steps to better secure their system to prevent future exploitation. While this will be painful at first it will encourage organizations around the world to more tightly control their systems.

Summary

Lani Kass, Director of the Air Force's Cyberspace Task Force stated "If you're defending in cyber, you're already too late… If you don't dominate in cyber, you cannot dominate in other domains. If you're a developed country, you can't conduct daily life [after a large scale cyber attack], your life comes to a screeching halt."[15] These statements are

[15] John Reed, *Officials Announce Cyber Command Will Take an Offensive Posture*, 5 October 2007,

accurate and show that the DoD is starting to more fully understand the need for cyber-attack capability. The Air Force is leading the DoD in this effort and is in the process of standing up a Cyber Command that will employ the full spectrum of cyber warfare. These efforts include developing a cyber attack capability that can be used against state sponsored and terrorist targets. This command and its capabilities are still under development and the Air Force is the only service actively seeking the capability to attack.

All military and civil defense agencies of the DoD must acquire the ability to wage cyber warfare and specifically must be able to strike terrorists with preemptive and retaliatory cyber attacks. The DoD must attack the terrorist ability to gain political power, train and command and control its operatives, and it must destroy the terrorists' capabilities to launch attacks against the US. The DoD's lack of cyber attack and active cyber defense capabilities limit the ability for the DoD to execute fundamentals of offensive warfare and to protect the nation from these threats.

2000 words

---

http://integrator.hanscom.af.mil/2007/October/10112007/10112007-14.htm, accessed 14 December 2007

Bibliography

Alberts, David S., Gartka, John J., Stein, Frederick P., *Network Centric Warfare.* DoD C4ISR Cooperative Research Program, 2000

Alexander, Yonah and Swetnam, Michael S., *Cyber Terrorism and Information Warfare*. Transnational Publishers, 2001, http://www.terrorismcentral.com/Library/Teasers/vatis.html, accessed 14 December 2007

Charbonneau, Louis. *Virtual Terrorist Training Camps Described*. 24 November 2007, http://www.pcworld.com/article/id,139897/article.html, accessed 14 December 2007

Department of Defense, Joint Publication 3-13. *Information Operations*. 13 February 2006, GL-6

Gieseke, Wolfram, *The Hacker Report*. Needham Heights: Data Beker Corp, 2001

Institute For Security Technology Studies At Dartmouth College, *Cyber Warfare, An Analysis Of The Means And Motivations Of Selected Nation States*. December 2004, http://www.ists.dartmouth.edu/projects/archives/cyberwarfare.pdf, accessed on 14 December 2007

Kolata, Gina, *Veiled Messages of Terror May Lurk in Cyberspace*. New York Times, 30 October 2001, http://query.nytimes.com/gst/fullpage.html?res=9B01E3D91730F933A05753C1A9679C8B63&sec=&spon=&pagewanted=all, accessed 14 December 2007

Myers, Lisa, *Web video teaches terrorists to make bomb vest*. 22 December 2004, http://www.msnbc.msn.com/id/6746756/, accessed 14 December 2007

Reed, John, *Officials Announce Cyber Command Will Take an Offensive Posture.* 5 October 2007, http://integrator.hanscom.af.mil/2007/October/10112007/10112007-14.htm, accessed 14 December 2007

Unknown, *Air Force Computer Emergency Response Team*. http://www.fas.org/irp/agency/aia/cyberspokesman/97aug/afcert.htm, accessed 14 December 2007

Unknown, *Joint Task Force - Global Network Operations*. http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html, accessed 14 December 2007

US Army Training and Doctrine Command, DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism.* 15 August 2005, IV-4

Venzke, Ben and Ibrahim, Aimee, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets.* Alexandria: Tempest Publishing, LLC, 2003, quoting Abu 'Ubeid al-Qurashi, *The Nightmares of America.* 13 February 2002. Quoted in US Army Training and Doctrine Command, DCSINT Handbook 1.02, Cyber Operations and Cyber Terrorism, 15 August 2005

Weimann, Gabriel, *www.terror.net: How Modern Terrorism Uses the Internet*. March 2004, http://www.usip.org/pubs/specialreports/sr116.html, accessed 14 December 2007