Cyber Attack: The Department Of Defense's Inability To Provide Cyber Indications And Warning

Subject Area DOD

EWS 2006

CYBER ATTACK: THE DEPARTMENT OF DEFENSE'S INABILITY TO PROVIDE CYBER INDICATIONS AND WARNING

Submitted by Captain D. M. Rock
CG # 5, FACAD: Major D. R. Wright
7 February 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 FEB 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Attack: The Department Of Defense?s Inability To Provide Cyber Indications And Warning	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)**	**9**	

CYBER ATTACK: THE DEPARTMENT OF DEFENSE'S INABILITY TO PROVIDE CYBER INDICATIONS AND WARNING

INTRODUCTION

The Department of Defense (DoD) is currently unable to provide Indications and Warning (I&W) of cyber attacks against the DoD Global Information Grid (GIG). In the cyber world there is generally very little forewarning of a threat. Most of the DoD's Computer Network Defense (CND) actions are reactionary, only initiated once an attack or probe has occurred. In order to provide warning of potential cyber attacks, capabilities within the DoD's Intelligence Community (IC) must be expanded. By improving the IC's collection capabilities in the cyber world through transforming traditional intelligence disciplines like Human Intelligence (humint) and Signals Intelligence (sigint) to better collect in a cyber environment IC will be able to provide I&W of future cyber attacks.

The anatomy of a cyber attack

Generally, a cyber attack will not be perpetrated from the place of origin. A hacker will jump through many

computers across the world before actually attacking a network. This method allows a hacker to disguise the true origin of the attack. Therefore, an attack from a hacker in a particular country might not appear to come from that country. If the IC does not know where the attack originated, who is responsible, and what their intentions are it will not be able to provide warning and help reduce or stop cyber attacks.

A significant amount of money and effort is being focused on Computer Network Operations (CNO), and, in particular, CND. One of these efforts resulted the creation of the Joint Task Force-Global Network Operations (JTF-GNO), which is the focal point for CND within the DoD.[1] The JTF-GNO mission is to provide a common defense of the GIG. However, this is no small task. The GIG is made up of more than 12,000 local area networks, roughly three million computers, and five million users.[2] Additionally, the services and agencies within DoD maintain their own networks and use a wide variety of equipment and procedures

[1] U.S. Strategic Command, "Joint Task Force-Global Network Operations," Factsheet, URL:<www.stratcom.mil>. Accessed 20 November 2005.

[2] Patrick Chrisholm, " Global Network Gaurdians," *Military information Technology*, URL:< www.military –information-technology.com>. Accessed 30 November 2005.

in the operation of these networks. The JTF has greatly increased coordination between DoD components and has operational control (OPCON) for CND missions. However, exercising their authority has proven difficult. Despite such efforts as the JTF-GNO there is a long way to go before the IC can provide I&W of cyber attacks. The ability to provide true I&W of cyber attacks will help ensure the protection of the DoD's critical infrastructure and allow the department to focus on its mission. Additionally, this forewarning will allow the DoD to greatly reduce the wasted man-hours and money that is spent reacting to attacks once they have already occurred.

WHAT ARE THE THREATS

The cyber threat to DoD comes from hackers. Hackers are categorized into two categories: state and non state-sponsored hackers. Both pose a significant threat to DoD information systems; however, their motivations for targeting the DoD can vary greatly. Additionally, the resources at their disposal vary considerably too.

Foreign governments and State-sponsored hackers

Due to the amount of resources that they have at their disposal, state–sponsored hackers pose the most serious threat to the DoD's information systems. Recently, series of ongoing intrusions into DoD and U.S. government information systems called Titan Rain highlight this. The Titan Rain intrusions, which are believed to have originated from China, were carried out in a methodical manner and required a highly sophisticated set of technical skills.[3] The hackers appeared to be conducting continuous 24 by 7 operations, which implied that they worked in shifts. A non state-sponsored hacker would not have the resources to conduct these types of operations. Foreign government use these types of operations to gather military and economic intelligence on the U.S.[4] The information gained on DoD networks could allow a foreign government to degrade, disrupt, or destroy information systems critical for the DoD to carry out its mission during a conflict.

Non state-sponsored hackers

Non state-sponsored hackers are a credible threat to DoD information systems as well. Typically, these hackers

[3] Time article need to get citation
[4] Government Accounting Office, *Economic Espionage: Information on Threat From U.S. Allies*, (Washington DC, 1996),

will target the DoD for ideological reasons or for the challenge of breaking into a difficult network. Although these hackers lack the resources of their state-sponsored counterparts they have shown the ability to successfully penetrate and cause significant damage to DoD networks.

WHAT IS THE INTELLIGENCE COMMUNITY DOING ABOUT IT

Today the IC is able to provide the CND community with information about a particular country or group's intent and capabilities in regard to offensive CNO (ie: can they attack successfully against DoD networks). However, recent studies have shown that not just non-friendly countries conduct exploitation against DoD networks, but allied countries are conducting significant activity as well.[5]

INDICATIONS AND WARNING IN THE "CYBER WORLD"

The DoD has to take a more aggressive collection posture in order to provide the I&W needed to prevent these widespread intrusions into its networks. Currently the majority of the DoD's collection capabilities reside on the

[5] Government Accounting Office, *Economic Espionage: Information on Threat From U.S. Allies*, (Washington DC, 1996),

networks in the form of intrusion detection systems, firewalls, and antivirus software. However, the focus should not be on its own networks, instead the DoD should be oriented outward. DoD intelligence collection should be focused on identifying threats before they intrude into the networks. This can be achieved through transforming traditional intelligence disciplines such as HUMINT and SIGINT to collect intelligence in the cyber world.

Sigint

Sigint is uniquely qualified to collect against cyber threats. The cyptologic field has been targeting communication networks for as long as there have been communication networks. Cyber operations are a natural extension of sigint and this is why most computer network operations are carried out by sigint personnel. By leveraging sigint assets to place collection sensors on the Internet and within enemy networks the IC will be able to identify threats before they penetrate DoD networks and exfiltrate sensitive and/or possibly classified information.

Humint

Humint operations, which are traditionally done through personal interaction can be utilized to support the defense of the DoD GiG. Instead of personal interaction, case officers can use the Internet to interact with hackers. This method of collecting information is far less costly than conventional humint operations, which require a lot of time and resources to recruit sources and establish background for case officers. Utilizing humint for supporting cyber operations can be invaluable for providing I&W of future cyber attacks.

INCREASED CAPABILITIES SOONER RATHER THAN LATER

The DoD has made great advances towards improving CND intelligence over the past few years. In May 2005, the JTF-GNO became fully operational. Additionally, the services are becoming more accepting the JTF's authority to dictate actions on their networks. However, DoD still has no ability to provide I&W of cyber attacks. General Cartwright, the Commanding Officer of U.S. Strategic Command recently stated that although the JTF-GNO has made a lot of progress there are still hundreds of intrusions

into DoD systems every day.[6] The DoD is becoming a more Network-Centric force relying heavily on networked information systems to perform its tasks. As the forces dependency grows on these networks to operate, the threat of cyber attacks increase as well.

The DoD needs to take immediate steps to focus its intelligence collection outward and transform traditional intelligence disciplines like sigint and humint to meet the challenges of an ever-increasing networked world.

Word Count: 1227

[6] Geoff Fein, " JTF Global Network Operations Achieves Full Operational Capability, " *C4I News*, 26 May 2005, 1.