STRATEGY RESEARCH PROJECT

CYBERTERRORISM VERSUS CYBERWAR: AT WHAT POINT DOES DEPARTMENT OF JUSTICE TURN OVER CYBER INCIDENTS TO The DEPARTMENT OF DEFENSE?

BY

DEBORAH P. GLASS
United States Department of State

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Cyberterrorism Versus Cyberwar: At What Point Does Department of Justice (DoJ) Turn Over Cyber Incidents to the Department of Defense?

by

Deborah P. Glass
United States Department of State

Professor Malcolm Cowley

Project Advisor

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

ABSTRACT

AUTHOR: Deborah P. Glass

TITLE: Cyberterrorism Versus Cyberwar: At What Point Does Department of Justice (DoJ) Turn Over Cyber Incidents to the Department of Defense?

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 27 CLASSIFICATION: Unclassified

The United States is increasingly dependent upon technology to the extent that every facet of the Nation's critical infrastructure (CI) depends on computer technology at some level. The conduct of future warfare, both offensively and defensively, is also increasingly technological. The realization that the US is extremely vulnerable to asymmetric warfare via the Internet and to acts of terrorism was part of the driving force behind the development of PDD 63. Because of the widespread dependence on the CI, consideration is being given to assigning ultimate responsibility over these interconnected systems to a single agency.

Currently the Federal Bureau of Investigation (FBI) has cognizance over items relating to terrorism. The Department of Defense has responsibility when it comes to acts of war. The line between terrorism and warfare over the Internet is ambiguous, as are the lines of authority. This paper will examine the definitions of terrorism and warfare where the Global Information Infrastructure and other components of our nation's CI are concerned. At what point, and by what mechanism should responsibility and authority be transferred from the FBI to the DoD? Should a different, perhaps even a new, agency be given ultimate response responsibility for attacks on the CI?

TABLE OF CONTENTS

CYBERTERRORISM VERSUS CYBERWAR: AT WHAT POINT DOES DEPARTMENT OF JUSTICE (DOJ) TURN OVER CYBER INCIDENTS TO THE DEPARTMENT OF DEFENSE?

The United States economy and its Department of Defense (DoD) are currently the strongest in the world. Both the economy and DoD are becoming increasingly dependent on cyber-based information systems and the Nation's Critical Infrastructure (CI). The CI are those "systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation"[1]. Among the systems comprising the National CI are telecommunication, energy, banking, finance, air traffic control, water, transportation and emergency service systems. The information infrastructures that operate and link these systems are increasingly at risk for attack through cyberspace.[2]

It is apparent, in light of the critical vulnerabilities within the CI, that it is highly probable that attacks on the United States could be launched through cyberspace in the form of cyber war or cyber terror attacks. Proven attacks and analysis of vulnerabilities of the many government systems, to include the DoD, resulted in the promulgation of Presidential Decision Directive (PDD) 63. PDD 63 gives a response role to Department of Justice (DoJ), DoD, the United States Secret Service (USSS), and other Federal Agencies.

U.S. policy currently designates DoJ as the agency with primary jurisdiction in the event an act of terrorism occurs within the United States, or againstU.S. entities or interests abroad. The Federal Bureau of Investigation (FBI), part of the DoJ, responded to the terrorist bombings in the cases of the USS Cole, and the Embassy bombings in Nairobi and Dar es Salaam. The DoD is the primary responsible agency when an act of war is perpetrated against the U.S. homeland, or U.S. interests abroad.

Cyber attacks are fraught with ambiguity and uncertainty. It is extremely difficult, and at times impossible, to determine who is responsible for an attack, where it comes from, and why it was launched. Cyber attacks can be routed through numerous servers around the world making it extremely difficult to determine the location from which an attack is launched. In instances where the attack is routed through countries with which the U.S. does not have diplomatic relations it is impossible to gain access to the Internet Service Provider (ISP). Once the launch point is established, it is still a difficult task to identify the attacker, and ultimately to establish the attacker's intent.

It is necessary to determine the identity, motive and intent of the attacker in order to classify an attack as a crime, an act of terrorism, or an act of war. The type of attack is relevant as well and may yield clues as to the intent of the attacker. Identify, motive and type of attack

are all critical pieces of the puzzle in determining whether the attack is an act of war, an act of terrorism, espionage, crime or malicious mischief. Just as important, this information is vital in determining which U.S. government entity is given jurisdiction in the investigation and response to a cyber attack.

This paper proposes that in keeping with stated missions a cyber attack determined to be an act of terrorism should be handed to the DoJ as the responsible agency and responder. Alternately, a cyber attack determined to be an act of war should be turned over to DoD as the agency charged with response once an FBI-led joint task force determines it to be such an act. It is critical that policy exists that clearly outlines the response to a cyber attack from the time it occurs. The response should begin with a joint investigation led by the FBI and assisted by other agencies. Simultaneously the Federal Emergency Management Agency (FEMA) should lead a crisis response as warranted by second and third order effects of the attack. The policy should clearly identify the circumstances in which the DoJ should turn a cyber war incident over to the DoD for further action.

BACKGROUND

There are many relevant issues the U.S. must deal with when a cyber-based incident occurs. Cyber attacks can be extremely complex. It is necessary to determine the exact nature of the threat. The attack could be categorized as a crime, an act of war, an act of terrorism, espionage, or malicious mischief. First the investigators must determine what type of attack is underway. There are several types of attacks that could seriously affect the CI. Common attacks are viruses or worms, denial of service, IP fragmentation, an ISP attack, spoofing and war dialers[3]. The launch point of an attack must then be established. The identity of the attacker must be ascertained and whether or not he is acting alone or as part of a group. Subsequently the motive and intent of the attacker must be determined. It is this piece of the puzzle that may determine the category of an attack. Additionally, the definitions of key terms and concepts must be modified to deal with cyber incidents. These issues must be dealt with prior to designating the agency best equipped and able to deal with the incident.

The Threat from Cyberspace

Computer systems today are increasingly vulnerable to cyber attacks through the use of the Internet. This is routinely illustrated by global viruses and worms like the I Love You virus and the denial of service attacks against Yahoo and other popular Internet web sites. The nations CI systems are not exempt from this vulnerability and the world situation makes the

threat to these systems significant. Cyber attacks like **Solar Sunrise**[4], an attack on the Pentagon's computer systems by three teenagers, alerted DoD to the vulnerability of computer systems within the military. Subsequently **Eligible Receiver's**[5] dramatic results fully opened the DoD leadership's eyes

To better understand the threat it is useful to understand the vulnerabilities that exist within the CI and how (in general) attacks can be carried out. There are two primary types of vulnerabilities within the CI. One vulnerability is to the information residing on the system. Information is vulnerable to theft (including espionage), erasure, falsification and alteration. An adversary might target personnel information, schedules, personnel movements, financial information, procurement information, designs, plans, medical information, customer databases and business proposals. The information system comprising the hardware and users, is the second vulnerability. The information system includes human factors, computers, nodes and links. The nodes within an information system include servers, routers, and satellites. Links include satellite links, microwave links and telephone cables[6]. Human factors include the ability of users to inadvertently, or purposely introduce viruses or worms by using infected magnetic media on the system. Human factors also include launching an attack from the inside. Hardware degradation or failure can result in information systems going off-line for a period of time. In many CI systems the down time could result in major inconvenience or inability to operate effectively causing serious second and third order effects.

No clear guidance or policy currently exists that delineates responsibility for cyber incidents within the federal government. The National Infrastructure Protection Center (NIPC) was created by PDD63. The NIPC is an interagency coordinating office within the FBI charged with gathering information on threats to the CI[7]. Several agencies are involved in protecting information systems as well as response to cyber incidents. These efforts are fragmented due to lack of communication and clear guidance regarding responsibilities. For this reason legislation was introduced with the purpose of consolidating counter-terrorism responsibility with a White House coordinating council. The Bill was passed by the House but defeated in the Senate due to Administration lobbying in opposition[8].

A single agency must be designated as the primary lead agency in response to terrorism incidents. This is to ensure there is a focal point for all investigative and response efforts as well as for information accumulating from various sources. Interagency coordination and cooperation must also be outlined to ensure all actors are fully aware of their roles, responsibilities and authority. The FBI's National Domestic Preparedness Center is currently the responsible government agency when dealing with acts of terrorism. The Center was

formed in the wake of the Oklahoma City and the World Trade Center bombings. The need for improving the response to terrorism was stated by Richard A. Clarke, the National Security Council's coordinator of counter-terrorism and computer security when he acknowledged that the FBI's National Domestic Preparedness Office is "badly broken"[9]. Efforts torespond to terrorism are fragmented within the government. The Government Accounting Office (GAO) currently addresses these issues, and also duplicates the FBI's interagency coordinating unit efforts[10]. Representatives from the GAO state that fragmentaton is a result of key interagency management functions being conducted by various agencies and departments without appropriate coordination and communication[11].

The Office of the National Coordinator for Security Infrastructure Protection and Counter-terrorism is the office that focuses on the protection of computer systems and the CI, attempting to engender a cooperative relationship between the government and private sectors to ensure the CI and associated systems are protected. The Office was established as a result of PDD 63 dated May 22, 1998. In the PDD there is no differentiation between terrorism, war, crime, mischief or espionage. The resulting ambiguity makes it more difficult to categorize attacks and assign responsibility. This ambiguity must be eliminated.

USS Cole Case Study – Terrorism or War

On 12 October 2000 the USS Cole endured a suicide bombing attack while anchored in the Port of Aden, Yemen. Two men approached the Naval vessel in a small boat, pulled alongside and detonated a bomb. A large hole was blown in the side of the ship killing 17 sailors and wounding 39[12]. The FBI dispatched anti-terrorist investigators within hours of the attack to work with Yemeni officials to determine who was responsible for the attack. Ultimately the identities of the suicide bombers were ascertained and others involved in the plot were arrested. In pursuing the terrorists the legal standards of Yemen had to be respected. Justice will take time as it did in the Pan Am 103 bombing, and in the cases of the embassy bombings in Dar es Salaam and Nairobi.

From the beginning President Clinton, and the nation, considered this attack to be an act of terrorism. Two men, acting on behalf of a terrorist group, carried out the bombing. One of the arrested suspects believes that the order to carry out the attack came from Osama Bin Laden, a known terrorist[13]. Bin Laden's intent and motive is to terrorize the U.S. in the ongoing effort to remove westerners from the Middle East. There are those that consider this attack to be an act of war. The argument is that the attack was carried out on a U.S. Navy ship, and is a

direct attack on the United States. Thus it is an act of war that demands an appropriate military response[14].

In the case of the US Cole it is clear that categorizing an attack is difficult due to ambiguity in definitions of terms. The responses to acts of war and acts of terrorism are different. An incident must be appropriately categorized in order to respond properly. This ambiguity makes categorizing cyber-incidents even more difficult.

Ambiguous definitions of War and Terrorism

To determine jurisdiction it is vital to differentiate between an act of war and an act of terrorism. Definitions for these terms are ambiguous and there is no agreement within the government as to the proper definition of each one.

Act of Terrorism

Several definitions for terrorism exist within the government as well as the global community. One source defines an act of terrorism as the "killing ofinnocent civilians for a host of possible reasons"[15]. An act of terrorism, as defined in PDD 39[16] (the FBI uses this definition) is a "violent act, or an act dangerous to human life which is in violation of the criminal laws of the United States, or any state, aimed at intimidating or coercing a government, the civilian population, or any segment thereof, in furtherance of political or social objectives". In the same vein, terrorism is defined as an "act of violence designed to achieve political objectives"[17]. The Department of State uses the definition "premeditated, politically motivated violence perpetrated against a non-combatant target by sub-national groups or clandestine state agents, usually intended to influence an audience"[18]. Finally, from the Webster's II Dictionary, terrorism is defined as "unlawful acts of violence committed in an organized attempt to overthrow a government; act of terrorizing, i.e. to reduce to a state of terror; intimidate through intimidation; terror – overwhelming impulse of fear"[19]. Though all of these definitions somewhat characterize a traditional act of terrorism, they are all insufficient when defining cyber terrorism. The definition of cyber terrorism must expand on the traditional definition, taking into consideration the attack medium as well as the immediate effects and second and third order effects of a cyber terror attack.

The primary effects of a cyber attack are not violent. It is the second and third order effects of a cyber attack that may result in death or destruction. A cyber attack targeting an

important infrastructure system may be a denial of service attack achieved either by overwhelming the system or taking it down. This attack could impair or disable the emergency response service, 911, where the system would be unable to handle incoming calls. In not being able to take calls and send response units, lives could be lost. The millennium Y2K preparations uncovered the vulnerability of chemical plants to loss of control systems in Cairo, Egypt. It is conceivable that loss of a critical control system could result in release of toxic gases from these plants affecting people in the densely populated city. Power grids, should the control systems be taken out of commission in the middle of winter, or the heat of summer, could result in loss of life. Thus, defining the act against a computer system as one of violence is inaccurate and consideration must be given to these second and third order effects.

The source of the attack is also important in defining terrorism. Rouge actors and groups often perpetrate terrorism. In some instances these terrorists may be acting with State approval. Although those without the means to wage a full war also consider terrorism warfare, for the purpose of defining terrorism these warriors will be considered terrorists.

For the purposes of this discussion then the definition of an act of terrorism through cyberspace shall be:

> An attack on a computer system through cyberspace by a rogue actor or group. The result or intention of the attack is to cause second and third order effects which result in injury or loss of life. The purpose of such an attack is to make a political statement, intimidate the subject, or influence the subject through intimidation or pressure from third parties such as a nation's people or the international media.

Act of War

As with terrorism, the definition of an act of war is varied among sources. One definition is an "act of violence against a U.S. military or government target"[20]. The Webster's dictionary states that "war is a contest between or among nations or states, or between different parties in the same state, carried on by force and with arms; any act of state hostility; enmity; strife; also a conflict or contest"[21]. As with terrorism, these definitions of war do not sufficiently describe an act of cyber war.

Again the primary effects of cyber attacks are not violent. The second and third order effects must be considered in this instance as well. First, an act of war will set the stage for

further attack either through cyberspace, or by conventional or strategic means. Denying service to Pentagon and White House computers as well as telecommunication systems for both locations, for example, may result in the U.S. being unable to respond to a nuclear attack due to the inaccessibility of the President or Vice President to order a retaliatory or immediate strike. In this case, the second and third order effects are not violent and do not result in injury or loss of life, but the stage is set for further attacks by a hostile state. It is essential then that in this war scenario several attacks occur either simultaneously or in a pattern to cripple the DoD for response, or the Government itself. Conceivably an act of war through cyberspace would attack numerous systems, for instance 911 systems regionally or across the entire U.S. which could potentially lead to significant loss of life. Other systems, like transportation, telecommunication, or air traffic control systems could also lead to injury or loss of life.

There are many acceptable definitions for traditional war, but for the purpose of discussing jurisdiction for cyber attacks, the following is offered as a working definition for an act of cyber war;

> Attacks, either simultaneously or sequentially, on several computer systems through cyberspace by a hostile state or significant opposition group within the country aimed at either setting the stage for further cyber or conventional attacks, or causing second and third order effects of significant injury or loss of life. The aim of the attack is to punish a country or overthrow its government, or directly force it to accede to a demand or alter its behavior.

Response Capabilities of Government Agencies

Several government agencies possess considerable resources and expertise to respond to cyber incidents. In all instances the response must be a cooperative effort between several government agencies. The question of primary jurisdiction and lead agency is significant. The United States Secret Service, the Department of Energy, Department of Commerce and other agencies could conceivably serve as lead agency on a cyber incident joint task force. The Department of Defense and the Department of Justice, specifically the FBI, are best suited for this role in most situations.

Department of Justice – The FBI

The FBI possesses significant resources to bring to bear in investigating a cyber incident. There is heavy investment in computer forensics and the tools are being proven in the field. The growing incidence of computer crime and other incidents provide FBI agents with real life experience, thus the resources that could be brought to bear in the face of a cyber attack are significant and proven.

The law enforcement capability of the FBI is an asset of immeasurable worth in the investigation stages of any cyber incident, be it an act of terrorism or an act of war. Numerous search warrants are typically necessary due to the circuitous and complex routing of cyber attacks. The FBI has the authority to acquire and act on these warrants within the United States. The presence of FBI field offices throughout the United States expedites the acquisition of warrants and subsequent contacts with and access to Internet service providers (ISP). This ability is unique in the FBI and is a vital asset needed to investigate a cyber incident.

The FBI also fosters relationships with law enforcement agencies in other countries across the globe. Most embassies have a Legal Attaché (LEGATT) office. Agents assigned to the LEGATT work with, in some instances very closely, host nations. The relationships are built through LEGATT assistance with organized crime efforts and access to training in various areas of law enforcement sending foreign law enforcement officials to training in the United States or to the training facility in Budapest, Hungary. A cyber attack's route will probably traverse ISPs in several countries. LEGATT agents, using these relationships with foreign law enforcement and judiciary officials, may be able to access ISPs in those countries, or enlist their assistance in accessing the ISPs.

The FBI also formally participates with the United Kingdom, Germany, Japan, Italy, Canada, France and Russia to improve cooperation in fighting high technology crimes. Among other things, the agreements between the US and these countries calls for developing faster methods to track down high technology criminals and to develop methods to preserve forensic computer evidence.

Department of Defense

The Department of Defense also possesses significant expertise and experience within its ranks to deal with cyber attacks. Computer forensic tools and expertise exist within the DoD to trace and investigate attacks. The Solar Sunrise incident, among others, provided DoD personnel the opportunity to gain field experience in tracking down and identifying cyber attackers.

There is also a significant DoD presence abroad. Nearly every embassy abroad houses a Defense Attaché Office (DAO), and in some locations there are regional CINC assets stationed within the embassies as well (Office of Defense Cooperation, Office of Military Cooperation). Additionally, military programs exist in many countries where training or assistance is given to host country militaries. It may be possible for DoD assets abroad to use the relationships that exist to access law enforcement and judiciary resources in that country in order to gain access to ISPs to further cyber attack investigations; however in these countries where both a DAO and a LEGATT exist the LEGATT normally has the responsibility and the connections.

The DoD is severely limited in its ability to perform law enforcement functions in the United States due to Posse Comitatas. In the event of a cyber attack the DoD would be unable to attain search warrants and access ISPs.

Federal Emergency Management Agency (FEMA)

FEMA is an invaluable resource in the event of a cyber incident where the second and third order effects of cyber attacks result in destruction or violence. FEMA's experience includes responses to floods, earthquakes, volcanic eruptions, hurricanes and a variety of other natural disasters as well as human situations (riots). The infrastructure, funding, experience, equipment and food and material stocks are available to respond to crisis and should take the crisis management lead.

National Infrastructure Protection Center (NIPC)

The NIPC could conceivably be designated as the lead coordinating agency in the event of a cyber attack. The NIPC was created as a result of PDD63 in the wake of Solar Sunrise and Eligible Receiver. The primary mission of the NIPC is to engender cooperation between the government and private sectors to ensure CI systems that are adequately protected fromcyber attack. The NIPC has no law enforcement capability or overseas contacts but the expertise and industry contacts make the NIPC a player and a candidate for a coordinator role.

Drug Enforcement Administration

The Drug Enforcement Agency, part of the DoJ, may be called in as a major player or a lead agency should a cyber attack be connected with drug trafficking. The DEA has the same advantages the FBI has as a law enforcement agency both domestically and abroad. Several DEA agents are stationed at embassies abroad and work directly with local law enforcement. The DEA would require FBI or DoD expertise to deal with the forensics in the investigation. In cases where drug trafficking is involved the DEA should play a supporting role.

Nation Homeland Security Agency (NHSA)

Increasingly there is a call in the Congress and within DoD to institute a Homeland Defense Agency. Former Defense Secretary William Cohen makes the argument that an entity must be created to respond to attacks on the homeland from inside, and out. He proposes that Commander in Chief for homeland defense be created and that the DoD is the logical parent organization for such an entity[22]. The Phase III report of the US Commission on National Security led by Senators Hart and Rudman also calls for a Homeland Defense organization. The Hart-Rudman recommendation is to form an agency built on FEMA and integrating U.S. Customs Service, the Border Patrol and the Coast Guard into a single agency. Customs, the Border Patrol and the Coast Guard would retain their respective identities but would be a part of the new agency. FEMA would coordinate interagency activities. An assistant Secretary position would be created to oversee DoD activities in this effort. The National Guard's primary mission would become Homeland Defense. As part of the recommendation for homeland defense agencies like the NIPC would be folded into the NHSA.

The Coast Guard does have some law enforcement ability to pursue a cyber investigation. They do not possess the forensic tools or investigative experience the FBI and DoD posses. Additionally, judicial contacts, and liaison with other law enforcement agencies are limited. None of the proposed groups for the NHSA have extensive ties overseas to assist them in pursuing leads abroad. Any response to a cyber attack, although possibly coordinated by an NHSA would require major assistance by other government agencies. Unless the NHSA builds these capabilities into the new agency, it should only be used as a coordinating agency or to perform the consequence management tasks FEMA would currently be assigned.

INTERAGENCY RESPONSE IN THE WAKE OF A CYBER ATTACK

In the wake of a cyber attack against a U.S. computer system it is vital to categorize the incident rapidly in order to determine who has jurisdiction and decide on the appropriate response type and level. This requires the investigating team to appropriately categorize the attack as a crime, espionage, terrorism, war, or mischief and then configure the team for response. The investigating team must comprise appropriate agencies to deal with the issues at hand, and should have lines of communication and authority to reach out to additional assets as requested. This is simple to state, but in practice difficult to implement due to the fact that the source, initiator, and intent of a cyber incident are difficult to ascertain.

Crisis Response and Consequence Management

The first priority in the wake of an attack is to restore service as soon as possible. The effected system's owner must bring the systems back on line. It is possible that government assistance may be required to recover the systems. Additionally, FBI or NIPC assistance may be necessary to preserve forensic evidence necessary for the investigation during system recovery. The longer a system is down, the greater is the chance that the second and third order effects may effect large populations and result in mass hysteria. Incapacitating the 911 system, air traffic control or telecommunication systems may result in deaths from the inability to get emergency assistance, or accidents due to defective or disabled air traffic control facilities. Power grids incapacitated during an intense cold spell could result in deaths, and possible mass hysteria. The first step in responding to a cyber attack is to bring the systems on-line. Should the second and third order effects of the situation warrant consequence management, it must commence immediately. These efforts must proceed alongside efforts to restore the systems and service, as well as the investigation. FEMA is well equipped to lead the consequence management effort.

The Investigation Phase

Determining the appropriate response to a cyber attack requires an intense investigation to answer the questions what, who, from where and why. Forensic evidence must be preserved during system restoration to facilitate the investigation. Both forensic and investigative experts

should be on-hand as system administrators work to recover from the cyber attack and bring their systems back on-line. Cyber attack investigations are extremely difficult and complicated.

Investigation Challenges

It is extremely difficult to investigate a cyber attack due to the complex environment in which it occurs. The questions what, who, where, and why must be answered before an incident can be categorized and an appropriate response devised. The initial question is what method is used in the attack. The attack could be a virus or worm, which affects the subject computers, theft of financial, proprietary, personal or sensitive information, or denial of service. This step can only be taken if an attack is detected. In many instances attacks on computer systems, especially information theft or modification, go unnoticed or unreported. Additionally, the full extent of the attack should be determined to learn the full ramifications of the attack and subsequently, to recover the computer systems and return to normal operations.

The question from where the attack is launched is far more difficult to ascertain. Cyber attacks can be routed through numerous ISPs around the globe. Attacks can be routed through countries with which the U.S. has no diplomatic relations in order to throw investigators off of the track. The complex routing will limit investigators' access to ISPs and makes the attack origin more elusive. The source of the attack is important in determining the level of importance placed on it by the U.S. government. In recent testimony before Congress it was stated that attacks originating in the U.S. are law enforcement concerns, whereas attacks originating from outside the U.S. borders are national security concerns[23]. This differentiation is not definitive since a cyber attack that affects national security could easily be launched from within the U.S. Several terrorists have been identified and apprehended within the U.S. Access to the country is not a limitation for those who would attack in this manner. On the flip side it is not difficult to initiate cyber crimes overseas. Several crimes have been committed from foreign servers that could not be considered threats to national security.

Once the origin of an attack is found, it then remains a strenuous task to determine the identity of the attacker. The very nature of the cyber world allows users to operate anonymously. In the case of Solar Sunrise, the identity of the Israeli teenager was gained through information from his protégé in California. Often the investigation cannot stop when the computer operator is identified and apprehended. At this point it becomes the investigator's task to determine if the individual is a member of a group or employed by a state and acting on its behalf. Many times the only way to determine whether or not an individual acted on his own

is through his own confession, or through witnesses who attest to his affiliation with a terrorist or a state organization.

The "why" is the most elusive, and arguably the most important question that investigators must answer in order to categorize a cyber attack. The intent and motive of an attacker is a vital piece of the attack puzzle. Cyber crime, espionage, terrorism, war and malicious mischief all have the same appearance at the outset. It is ultimately the attacker's intent that defines the nature of the attack. An attack against a financial institution may be motivated by greed in a criminal act. It could also be motivated by a desire to effect the financial institution that may, in turn, affect the government. For instance if several institutions were affected almost simultaneously or in a concerted sequential effort the effect could possibly be loss of confidence in the industry and possibly a run on the institutions. The effects in the financial market could result in loss of confidence in the government itself. Theft of information over cyber space may be perpetrated by a criminal in a quest for monetary gain, or by a hostile intelligence service that could use the information, especially personal information, for recruiting spies.

To answer one question is to solve only part of the puzzle. All of the pieces must be in place to arrive at the correct conclusion and ultimately categorize an attack. For example, an attack on many major DoD systems in a systematic manner would, on the surface, appear to be an act of war. As seen in Solar Sunrise though, a seemingly warlike, aggressive attack turned out to be a teenager interested in seeing what he could do to a DoD computer. This is a prank that appears to be something more. Only when the questions where, who, why and what are answered is the proper conclusion reached.

Investigative Capabilities in the FBI and DoD

The investigator needs tools to track through cyberspace to find the answers to the vital questions of what, when, who and why. To accomplish this mammoth task the investigating agency must have the ability to acquire necessary warrants for ISP access to servers and information. Several agencies possess the forensic tools necessary to trace an attack through cyberspace. The FBI has the advantage of having law enforcement authority that is required to gain necessary warrants and access. Additionally, only the FBI has pervasive judicial relationships through contacts in the numerous field offices and resident agents throughout the country. These contacts will facilitate warrant acquisition and reduce the investigation time. The Department of Defense, with a waiver to the Posse Comitatas Act of 1878, could conceivably perform law enforcement activities. It is stated in 18 U.S.C. 1385 that military

forces cannot be used to "execute the laws" unless "expressly authorized by the Constitution or Act of Congress". To enable the military to participate in a law enforcement role in a cyber attack investigation the Congress would have to pass an act granting a waiver, or the President would issue an Executive proclamation. This step takes time and could result in the loss of vital forensic evidence. The law enforcement expertise and the network residing between the military and the judiciary, and the military and law enforcement agencies are far less extensive than those engendered within the FBI. Additionally, public perception may be severely impacted should an exception to Posse Comitatas be provided in an investigation.
Access to foreign ISPs is a major obstacle that must be overcome to see an investigation through to a successful conclusion. Because a cyber attack will more that likely be routed through numerous ISPs all over the world, gaining access to foreign ISPs, either directly or through host country assistance, is necessary. Although both the FBI and DoD have close ties with counterparts abroad, it is likely that the law enforcement connections will be far more advantageous in gaining the needed access and subsequent legal assistance and cooperation should a perpetrator be identified.

It appears a cyber attack investigation falls squarely in the realm of the FBI. The resources and expertise, ability to acquire necessary warrants through judiciary and local law enforcement relationships, and the ability to gain access, directly or indirectly, to foreign ISPs weight the lead investigator scale heavily toward the FBI. As part of a responding interagency joint task force, jurisdiction, authority and responsibility should be placed on the shoulders of the FBI.

The Retaliation/Justice Phase

The final categorization of an attack resulting from the investigative phase will determine the appropriate response to a cyber incident. It is also in the this phase that although the DoD may be called upon to make a retaliatory strike after an act of terrorism, in this case leadership of the task force should remain with the FBI. Should the incident be declared an act of war the DoD should take on the leadership role.

Legal responses to terrorist incidents may be extremely difficult depending on the location of the individual or group responsible for the attack. The bilateral agreements between the U.S. and the country in question may or may not include extradition of a terrorist, or even access to the suspect once he has been identified. It is possible that the country from which an attack is launched may not have rule of law. In these cases the perpetrator may never be brought to justice. It is also possible that the attacker is a minor player within a major terrorist group, or an

affiliated group within the larger terrorist organization. To bring the single player to justice does not complete the response. It is in these cases where a military response may be desirable as was the case following the Embassy bombings in Nairobi and Dar es Salaam. Individuals were arrested for their participation in the bombings, but military strikes were executed against a pharmacy in Khartoum, Sudan and against the location of an Osama Bin Laden camp in Afghanistan. Although the organizations were not eliminated, or even severely effected, the U.S. did send a message that the nation would fight back against terrorism. It is conceivable that this is the type of response the Administration will call for when a cyber incident is categorized an act of terrorism.

In the event an incident is categorized an act of war, the DoD must take the response lead, taking both a defensive and an offensive stance. The military must always look outward to ensure a direct conventional or strategic attack on the U.S. homeland does not occur. It is best to prevent an aggressor from commencing a strike against the physical boundaries of American homeland. This is the defensive stance that must complement an offensive stance. The military must prepare for active response to an act of cyber war should the National Command Authority (NCA) determine that it is necessary. Orders from the NCA may result in strategic or conventional warfare. The NCA orders may also be for execution of Information Warfare against the aggressor. In all instances, once a cyber attack is categorized an act of war, jurisdiction, authority and responsibility should be given to the DoD.

RECOMMENDATION

A comprehensive policy that clearly outlines the appropriate response to a cyber incident should be promulgated. Lead agencies and joint task force participants for the three phases, consequence management, investigation and retaliation/justice must be identified and appropriate authority bestowed on the agency to meet the responsibilities of the role. FEMA should be identified as the primary agency in dealing with consequence management in situations where second and third order effects include domestic damage and warrant such a response. The FBI should be designated the lead agency in all cyber attack investigations. The FBI should retain leadership in the retaliatory phase if an attack is categorized an act of terrorism. They are best suited to negotiate the legal forest to bring terrorists to justice. The National Command Authority may order a military strike in response to a terrorist attack, like the attack on the pharmaceutical company in Khartoum, Sudan and the terrorist camp in Afghanistan. In this case the DoD would take the task, but overall leadership of the incident

should remain with the FBI. The DoD should take the helm If an attack is categorized an act of war and the National Command Authority decides an appropriate military response is in order. The appropriate response may be an Information Warfare Operation conducted against the attacker, a single conventional attack, numerous conventional attacks, or even a strategic strike depending on the severity of the cyber attack.

CONCLUSION

The U.S. is becoming more and more vulnerable to asymmetric warfare as it becomes more dependent on information systems. Preventing cyber attacks should be a top priority of the government and private industry. In the event a cyber attack occurs it is a difficult task to determine who the attacker is and the motives for the attack, from where an attack is launched, and exactly what type of attack has occurred. Intense investigation is required to answer these questions and to categorize an incident appropriately. Whether an incident is categorized as crime, espionage, mischief, terrorism or warfare will determine the appropriate response and responding agency.

The first step when any cyber attack has occurred is to recover the system and services provided by the system as well as provide aide to those who may have been injured by the immediate second order effects. It is essential that valuable forensic evidence be preserved throughout the system recovery to assist the investigators in their efforts. Consequence management response may be necessary at the same time to address second and third order effects of the attack. These effects may include loss of emergency 911 capability, power, air traffic control, and communications. Loss of these systems could lead to death and destruction, and ultimately to mass hysteria should the service be unavailable for a prolonged period.

To perform the investigation it is vital that the lead agency on a joint task force have law enforcement authority and appropriate networks to acquire warrants and gain access to ISPs. Investigators must have the requisite tools and expertise to trace a cyber incident. Finally, the investigating agency must have foreign contacts to gain access to foreign ISPs should the route transit other countries. The FBI is the agency that should be assigned lead throughout an investigation up to the point where a categorization is concluded.

The attack categorization will determine the appropriate response. The FBI should follow through with the retaliation/justice phase if an incident is categorized as an act of terrorism if it is possible. Laws of the country where the attack is launched must be respected and upheld.

The President and NCA may decide a strong military response is appropriate at which point the DoD would perform the task, but the FBI would continue as the lead task force agency. In the event an incident is categorized an act of war the DoD should be designated the lead task force agency and configure military resources for both a defensive and an offensive stance. Only with this response will the U.S. be adequately be protected by an aggressive party intent on waging war against the United States.

It is not "if" a cyber attack is going to occur, it is when. President Clinton is on record as stating,

> "Our security is challenged increasingly by nontraditional threats from adversaries, both old and new, not only hostile regimes, but also international criminals and terrorists who cannot defeat us in traditional theaters of battle, but search instead for new ways to attack by exploiting new technologies and the world's increasing openness"[25]

An attack will occur at some point in the future and the U.S. must be ready to respond quickly and effectively. To that end, a clear U.S. policy should be promulgated as a National Security Decision Directive[24] that outlines this type of response and provides the joint task force constitution and responsibilities of each participant.

6909

ENDNOTES

[1] Dr. Gerald L. Kovacich and William C. Boni, High-Technology-Crime Investigator's Handbook Working in the Global Information Environment (Boston, MA: Butterworth Heinemann, 2000),49.

[2] PDD 63: The Clinton Administration's Policy on Critical Infrastructure Protection, (1998), 2.

[3] Ibid, 80-81.

[4] Attack against Pentagon computer systems, February 1998. Perpetrated by two California teenagers, and an 18 year old Israeli. Considered malicious mischief. The two teenagers pleaded guilty and received a fine, and a sentence of three years probation and 100 hours of community service. The Israeli teenager's case is still pending. Ehud Tenebaum is currently assisting the effort to protect Israeli computer systems from Palestinian cyber attacks.

[5] Red team exercise aimed at exposing vulnerabilities in DoD systems.

[6] Joint Doctrine for Information Operations, Joint Pub 3-13, October 1998, III-1/2.

[7] Congress, Senate. Subcommittee on Government Management, Information and Technology, Testimony of John T. Spotila, Administrator, Office of Information and Regulatory Affairs Office of Management and Budget. 26 July 2000; available from www.house.gov/reform/gmit/hearings/2000haerings/000726cybersecurity/000726js.htm; Internet; accessed 28 September 2000.

[8] Vernon Loeb, "After Counter terrorism Bill Fails, Nation's Preparedness is Debated", Washington Post, 9 October 2000, pg 21.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Orders From Osama,"; available from <abcnews.go.com/sections/world/DailyNews/yemen010108>; Internet; accessed 10 February 2001.

[13] Ibid

[14] Seth Cropsey, "War not Terrorism," Washington Times, 16 October, 2000.

[15] "Ibid.

[16] PDD 39 – Terrorism Incident Annex to the Federal Response Plan; available from <www.fas.org/irp/offdocs/pdd39_frp.htm>; Internet.

[17] Steven A. Hildreth. "Cyberwarfare," CRS Report for Congress order Code RL30735, page 14.

[18] Dr. Gerald L. Kovacich and William C. Boni, High-Technology-Crime Investigator's Handbook Working in the Global Information Environment (Boston, MA: Butterworth Heinemann, 2000), 65.

[19] Anne H. Soukhanov, editor, Webster's II New Riverside Dictionary, (Boston MA: The Riverside Publishing Company), 1195.

[20] "Seth Cropsey, "War not Terrorism," Washington Times, 16 October, 2000.

[21] Anne H. Soukhanov, editor, Webster's II New Riverside Dictionary, (Boston MA: The Riverside Publishing Company), 1300.

[22] Gail Kaufman, Cohen Stresses the Need for Homeland Defense, InsideDefense.com, October 3, 2000.

[23] Congress, Senate,Testimony by Richard C. Schaeffer, Jr. Director, Infrastructure and Information Assurance Office of the Assistant Secretary of Defense, Subcommittee on Government Management, Information and Technology, July 26, 2000.

[25] Judge William H. Webster and Arnaud de Borchgrave, "Cyberccrime... Cyberterrorism... Cyberwarfare; available from www.csis.org/pubs/cyberfor.html. Internet; accessed 15 March 2001.

[24] National Security Presidential Directive (NSPD) is President Bush's designation as a replacement for Presidential Decision Directives. (PDD)

BIBLIOGRAPHY

PDD 63: The Clinton Administration's Policy on Critical Infrastructure Protection. (1998).

Joint Doctrine for Information Operations. Joint Pub 3-13, October 1998, III-1/2.

Congress, Senate. Subcommittee on Government Management, Information and Technology, Testimony of John T. Spotila, Administrator, Office of Information and Regulatory Affairs Office of Management and Budget. 26 July 2000; available from www.house.gov/reform/gmit/hearings/2000haerings/000726cybersecurity/000726js.htm; Internet; accessed 28 September 2000.

Loeb,Vernon. "After Counter terrorism Bill Fails, Nation's Preparedness is Debated." Washington Post, 9 October 2000, pg 21.

Orders From Osama." Available from <abcnews.go.com/sections/world/DailyNews/yemen010108>. Internet; accessed 10 February 2001.

Cropsey, Seth . "War not Terrorism." Washington Times, 16 October, 2000

PDD 39 – Terrorism Incident Annex to the Federal Response Plan. Available from <www.fas.org/irp/offdocs/pdd39_frp.htm>. Internet.

Hildreth, Steven A. "Cyberwarfare." CRS Report for Congress order Code RL30735, page 14.

Soukhanov,Anne H, editor. Webster's II New Riverside Dictionary. (Boston MA: The Riverside Publishing Company), 1195.

Kaufman,Gail. Cohen Stresses the Need for Homeland Defense. InsideDefense.com, October 3, 2000.

Congress, Senate,Testimony by Richard C. Schaeffer, Jr. Director, Infrastructure and Information Assurance Office of the Assistant Secretary of Defense, Subcommittee on Government Management, Information and Technology, July 26, 2000.

Kovacich, Dr. Gerald L and Boni.William C.. High-Technology-Crime Investigator's Handbook Working in the Global Information Environment. Boston, MA: Butterworth Heinemann, 2000.

Webster, Judge William H. and de Borchgrave , Arnaud, "Cyberccrime... Cyberterrorism... Cyberwarfare. Available from <www.csis.org/pubs/cyberfor.html>. Internet. Accessed 15 March 2001.