U.S. Security Strategy toward North Korea’s Cyber Terrorism

Sunny Lee
Director of IKUPD
Institute for Korea-U.S. Political Development

www.ikupd.org
ikupd@yahoo.com
Tel: 702-328-0078
U.S. Security Strategy toward North Korea’s Cyber Terrorism

Sunny Lee

Abstract

U.S. authorities would find out the origin of the widespread cyber attack coming from North Korea that overwhelmed government web sites in the U.S. and South Korea, even though it would be difficult to definitively identify the attackers quickly. The powerful attacks that targeted dozens of government and private sites underscored how the Korea and U.S. government both should prepare to block such multipronged assaults.

North Korea’s cyber terrorism is a new challenge on the top of military terrorism that it will focus on developing high techniques with much advanced methodology for effective outcomes. North Korea has been caught in faint with a shocking cyber-offensive that has broad implications for the North Korea’s drive to perfect its ability to deliver weapons of mass destruction to carefully selected targets in Japan, South Korea or possibly the U.S. North Korea can ultimately stage artillery and missile attacks on major U.S. bases in South Korea with a full-scale cyber-offensive capability and even conduct its cyber attacks toward the U.S. territory.

This paper analyzes all possible aspects of cyber terrorism by North Korea and suggests strategic models to beat up its fundamental attacks in U.S. military strategy.

Keyword: North Korea, New Military Technique, Cyber Terrorism, U.S. Military Strategy
I. What is Cyber-Terrorism?

The U.S. is getting harder dilemmas in its security strategy by cyber-terrorism that persistent computer security vulnerabilities may expose U.S. critical infrastructure and government computer systems to possible cyber attack by terrorists, affecting economy, military and other areas of national security. This possible cyber capabilities of terrorists and sponsoring nations, describes how computer security vulnerabilities might be exploited through a cyber terror attack and raises some potential issues in U.S. cyber-terror strategy.

Now, as such, the international society gets encountered new security dilemma by cyber-terrorism which requires drastic military techniques to defeat. Cyber terrorism is new concept of military strategy that the FBI defined it as the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-

---

national groups or clandestine agents. Cyber-terrorism could thus be defined as the use of computing resources to intimidate or coerce others. An example of cyber-terrorism, if North Korea hacks military information system of the U.S. or South Korea and make them disable when it triggers war on the Korean Peninsula, North Korea will absolutely be winning the position in the cyber warfare.

The U.S. government has banned the uploading and downloading of open source code to residents of a handful of countries on its sanctions list, which includes North Korea. The STPI report also said that North Korea has launched a cyber-war unit that targets sites in South Korea and the U.S. In July, 2009 South Korea experienced a wave of cyber-attacks which attempted to paralyze a number of websites. U.S. websites including the Pentagon and the White House were also targeted. Reports suggested that the attacks might have originated in North Korea that North Korea has screwed up international security with nuclear weapons but cyber-terrorism is more dangerous in variable aspects beyond conventional military weapons techniques.

1. Cyber Terrorism’s Era

General John Gordon, the White House Homeland Security Advisor at the RSA security conference in San Francisco, CA Feb. 25, 2004 indicated that if someone detonates a bomb it causes bodily harm to innocent people or hacks a web-based IT system in a way it could, for instance, take a power grid offline and result in blackout. The result is ostensibly the same as stating that the potential for a terrorist cyber attack is real. As such, by the use of the internet the terrorist can affect much wider damage or change to a country than one could killing some people. From disabling a countries military defenses to shutting off the power in a large area, the terrorist can affect more people at less risk, than through other means.

Computers and the internet are becoming an essential part of daily life by individuals and societies for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life. Such a tremendous role of computers stimulated criminals and terrorists to make it their preferred tool for attacking their targets. The internet has provided a virtual battlefield for countries having problems with each other such as Taiwan against China, Israel against Palestine, India against Pakistan, China against the U.S., and many

---

other countries.

This transformation in the cyber-terrorism from traditional methods to electronic methods is becoming one of the biggest challenges to modern military technology. In order to combat this type of terrorism a lot of effort should be done at the personal level, the country level, the regional level, as well as the international level to fight against this transnational type of crime.

2. Cyber Terrorists

Cyber terrorist prefer using the cyber attack methods because of many advantages for it.

1) Cheaper than traditional methods
2) Difficult to be tracked
3) Hiding personalities and location
4) No physical barriers or check points to cross
5) From anywhere in the world
6) Attacking a big number of targets
7) Affecting a large number of people or countries in war

The most dangerous terrorist group used to be Al-Qaeda which has been considered as the first enemy toward the U.S. The U.S. official data from computers seized in Afghanistan indicate that the group has scouted systems that control American energy facilities, water distribution, communication systems, and other critical infrastructure. As well, after April 2001 collision of U.S. navy spy plane and Chinese fighter jet, Chinese hackers launched Denial of Service (DoS) attacks against U.S. web sites.

The second half of the year 2002 showed that the most dangerous nation for originating malicious cyber attacks is the U.S. with 35.4% of the cases down from 40% for the first half of the same year. South Korea came next with 12.8%, followed by China 6.2% then Germany 6.7% then France 4%. The UK came number 9 with 2.2%. Israel was the most active country in terms of number of cyber attacks related to the number of internet users.

Contemporarily, North Korea is the worst cyber terrorist country in the international society. North Korea’s cyber terrorism as a kind of new military technique is not only focused on South Korea but also the U.S. U.S. authorities would find out the origin of the widespread cyber attack coming from North Korea that overwhelmed government web sites in the U.S. and South Korea, even though it would be difficult to definitively identify the attackers quickly. The powerful attacks that targeted dozens of government and private sites underscored how the Korea and U.S. government both should prepare to
block such multipronged assaults. For instance, while Treasury Department and Federal Trade Commission web sites were shut down by the software attack, which lasted for days over the holiday weekend, others such as the Pentagon and the White House were able to fend it off with little disruption.

3. Cyber Attacks

North Korea’s cyber terrorism is a new challenge on the top of military terrorism that it will focus on developing high techniques with much advanced methodology for effective outcomes. North Korea has been caught in faint with a shocking cyber-offensive that has broad implications for the North’s drive to perfect its ability to deliver weapons of mass destruction to carefully selected targets in Japan, South Korea or possibly the U.S. If North Korean attacks the West or Yellow Sea or possibly across the DMZ between the two Koreas, it can initiate an audacious cyber-offensive over the weekend and revive it to peak levels by mid-week.

Moreover, North Korea recently linked the cyber-offensive directly to a recent flurry of missile tests as well as the test of an underground nuclear device that their security is integrally tied to cyber-warfare. While miniaturizing nuclear warheads to fit on the tips of missiles, part of an effective confrontation with the U.S. war machine could disable U.S. information systems by North Korea’s cyber terrorism. This strategy fits in integrally with tests of atomic devices in North Korea. North Korea ultimately can stage artillery and missile attacks on major U.S. bases in South Korea in tandem with a full-scale cyber-offensive. The cyber-offensive was enough of a shock to sublimate concerns about North Korean proliferation of weapons ranging from rifles to missiles to components for nuclear devices.

II. North Korea’s Ventures toward Cyber Terrorism

North Korean leader, King Jongil recently reinforced to train cyber hacking troops as the top national military strategy. Especially, if North Korea can temporarily paralyze or disable other country’s electric military systems as soon as it triggers the war, it will definitely lead to win. In fact, North Korea mostly depends on conventional military that is not much effective in the contemporary war. North Korea’s nuclear weapons and missile techniques comparing to South Korea would not be considered as the comparable status that the U.S. can smash anytime.

Even though North Korea announced it possess nuclear weapons and conducted nuclear tests, the U.S. would not consider its overall military capability. However, North Korea newly initiated cyber terrorism
toward the U.S. that North Korea attacked and disabled websites of the White House, the Treasury Department and the Defense Department by cyber terrorism. Now North Korea’s military cyber terrorism seems more dangerous in cyber warfare in advanced cyber techniques that North Korea will strive to reinforce to take advantage of actual military war.

### 1. North Korea’s Cyber Military Capacity

North Korea still absolutely counts on conventional military capacity. But it shows how North Korea has concentrated on developing cyber techniques for the new military strategy to challenge the U.S. as well as South Korea. North Korea might be decades behind development, but when it comes to cyber warfare, the nation is growing an elite army of hackers, seeking out the best of the best computer prodigies, showering them and their families with lavish lifestyles, and effectively training them.

Technolytics, with support from Intelomics and Spy-Ops, created a cyber threat matrix by the international standard in 2007. It measured intent and capabilities of six potential adversaries of the U.S. that North Korea is in very challenging status after China and Russia in Northeast Asia. North Korea’s cyber threat is getting worse as it reinforcing training systems.

#### CYBER THREAT MATRIX

<table>
<thead>
<tr>
<th>Country</th>
<th>Estimated Military Spending</th>
<th>Intent</th>
<th>Estimated Threat</th>
<th>Current Capabilities</th>
<th>Basic Data Weapons</th>
<th>Intermediate Data Weapons</th>
<th>Advanced Data Weapons</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>$55.50</td>
<td>5.0</td>
<td>High</td>
<td>4.2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Iran</td>
<td>$9.70</td>
<td>4.0</td>
<td>Elevated</td>
<td>3.4</td>
<td>Yes</td>
<td>Limited</td>
<td>No</td>
</tr>
<tr>
<td>Libya</td>
<td>$1.30</td>
<td>3.0</td>
<td>Moderate</td>
<td>2.5</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>North Korea</td>
<td>$5.20</td>
<td>3.0</td>
<td>Elevated</td>
<td>2.8</td>
<td>Yes</td>
<td>Limited</td>
<td>No</td>
</tr>
<tr>
<td>Russia</td>
<td>$44.30</td>
<td>5.0</td>
<td>High</td>
<td>4.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Syria</td>
<td>$8.80</td>
<td>3.0</td>
<td>Moderate</td>
<td>2.2</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

*Estimated Military Spending is in Billions of U.S. Dollars*

*Rating Scale: 1 = Low 2 = Limited 3 = Moderate 4 = High 5 = Significant*

---

4 The Technolytics Institute (Technolytics) was established in 2000 as an independent executive think tank. The institute consults for the U.S. government, as well as governments of other nations, on information security and information security management. Intelomics and Spy-Ops are also security management consulting organizations for the U.S. government.
North Korea has been building up a hacking squad since 1986. The reclusive nation turned to reinforce electronic warfare tactics all the more since economic hardships during the 90s led to difficulties in expanding its conventional weapons arsenal. But North Korea’s General Bureau of Reconnaissance (unit 586—another name)\(^5\) started to conduct cyber terrorism projects as the center of terrorism, which oversees all international espionage operations, also specializes in electronic warfare. The South Korean Defense Ministry pointed out North Korea’s Reconnaissance General Bureau as the most likely suspect of attack on the Cheonan Warship on March 26, 2010.\(^6\)

North Korea in 2011 raised the status of its cyber warfare unit under the Reconnaissance General Bureau and increased the number of troops in the unit from 500 to about 3,000.\(^7\) It trained total 16,500 terror troops and charged 10,000 with cyber terrorism. As well, North Korea has supported training hackers and cyber warfare through higher education. It is scouring its universities for computer prodigies to send overseas for training as part of a plan to expand its cyber warfare unit, underscoring the increased risk of cyber attacks.\(^8\)

Five major universities have trained cyber hackers each year. Furthermore, Mirim University concentrates on training cyber warfare tactics by Russian professors. In order to develop North Korea’s cyber terrorism capabilities and hacking technology through the cultivation of professional hackers, Mirim University, which changed its name to Kim Il Political Military University in 2000 and is known as a “secret university,” was founded in 1986. This university, affiliated with the Ministry of the People’s Armed Forces, educates some 100 world-class hackers every year and appoints them as military officials to hacking units under the General Bureau of Reconnaissance of the Ministry of the People's Armed Forces.

---

\(^5\) The Reconnaissance General Bureau is one of the KPA(Korean People’s Army)’s three most powerful organs. The general bureau is an integration of the reconnaissance department of the North Korean defense ministry, the “operations department” which developed infiltration routes for secret agents and “Room 35” in charge of international intelligence under the Workers’ Party. The general bureau now consists of six bureaus for operations (Bureau 1), reconnaissance (Bureau 2), overseas intelligence (Bureau 3), inter-Korean talks (Bureau 5), technology or cyber terrorism (Bureau 6) and for support of other divisions (Bureau 7).


Table 1

North Korea’s Cyber Warfare Training Status

<table>
<thead>
<tr>
<th>Institute</th>
<th>Training</th>
<th>Faculty</th>
</tr>
</thead>
</table>
| Mirim University (Pyongyang Automation University) | - electronic warfare tactics
-a hundred hackers every year                    | 25 Russian professors from the Frunze Military Academy   |
| Amrokgang College of Military Engineering      | hackers                                            |                                                          |
| The National Defense University                | hackers                                            |                                                          |
| The Air Force Academy                          | hackers                                            |                                                          |
| The Naval University                           | hackers                                            |                                                          |

Since North Korean authorities have been developing the nation’s cyber terrorism capabilities by
training professional hackers since the mid-1980s, it is possible and even likely that indiscriminate cyber attacks, which could cause more serious damage, may be launched in order to cause chaos in South Korean society. The reason for this is because the Internet is a much easier tool of attack to use than other tools of attack.

According to direct instructions handed down by Kim Jong Il in 1998, for each base of the People’s Army, military authorities have implemented high-tech information and computer education. After the Kosovo war, Kim Jong Il reportedly commented that the war of the 20th century was a war of oil and bullets, but the war of the 21st century is one of intelligence.

2. Current Techniques of Cyber Terrorism

South Korean president and defense ministry home pages appear to be unavailable on July 8, 2011.

If North Korea launched a nuclear weapon, the U.S. would know exactly where it launched from and where to go. Terrorists, however, are much more elusive individuals, and therefore much harder to capture. It can deter countries far more than it can deter terrorists. It seems impossible to prevent future cyber attacks similar to the one that has been targeting dozens of Web sites in the U.S. and South Korea since the July 4 holiday weekend, 2009. Called directed denial-of-service attacks, or DDoS, they are easy

to carry out, and the method is simple: Bombard the servers hosting a particular Web site with so many requests for information that the servers become overwhelmed and the site goes offline.10

There is no way currently known that can prevent these kinds of things from occurring, Eugene H. Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security, told FOXNews.com. These attacks rely on the poor protection and compromises of computer systems around the world. In this instance, malicious computer programmers, working for North Korea, would have started by infecting thousands of computers running Microsoft Windows with a computer virus. A rogue programmer would then have been able to "herd" the PCs into a virtual networked computer, or "botnet," that he could command to do whatever he wanted. When the attack began, the "bot herder" would have directed his botnet to begin requesting information from the Web servers, much as you do when you go to a Web site.

A recent attack paralyzing the computer system of Nonghyup Bank in South Korea has raised fears about North Korea’s cyber terrorism capabilities, especially following the past North Korean DDoS attacks on July 7, 2009, and March 4, 2011.11 Although the two previous DDoS attacks only resulted in confusion for users of major governmental websites, the Nonghyup attack has shocked analysts due to the real damage it has caused to the financial property of individual South Koreans. The South Korean National Intelligence Service stated that the main culprit behind the Nonghyup computer system attack was the General Bureau of Reconnaissance, which was also behind the Cheonan shinking in March and the Yeonpyeong Island shelling in November 2010. The General Bureau of Reconnaissance was formed through the merger of the Operation Department in charge of the infiltration and assistance of spy escorts, the No. 35 Department in charge of collecting information on South Korea and other countries, and the Bureau of Reconnaissance of the Ministry of the People’s Armed Forces in February 2009.

Agents of the 121 Office, a cyber terrorism unit under the General Bureau of Reconnaissance, possess world-class hacking ability. South Korea’s intelligence authorities also confirm that there are around 1,000 cyber warriors in the General Bureau of Reconnaissance and that bases have been set up in several locations in China to carry out hacking operations. Additionally, it has been reported that North Korean hackers have been recorded approaching the websites of the U.S. CIA and Department of State in recent

---

years. North Korea’s hackers apparently have ten times the strike capability of South Korea’s. North Korea is, furthermore, currently at a stage where it can directly attack South Korea's infrastructure through the use of cyber terrorism. Hackers working in perfect cooperation and being led by a coherent command system are much more dangerous than individual hackers and that North Korea’s hackers carry out operations from China and other third countries, which also adds to difficulties in uncovering their activities. North Korea’s ability is no less than that of China or Iran, which are both powerful nations when it comes to waging cyber war.

3. Main Targets

North Korea’s cyber terrorism as a kind of new military technique is not only focused on South Korea but also the U.S. U.S. authorities would find out the origin of the widespread cyber attack coming from North Korea that overwhelmed government web sites in the U.S. and South Korea, even though it would be difficult to definitively identify the attackers quickly. The powerful attacks that targeted dozens of government and private sites underscored how the Korea and U.S. government both should prepare to block such multipronged assaults. While Treasury Department and Federal Trade Commission web sites were shut down by the software attack, which lasted for days over the holiday weekend, others such as the Pentagon and the White House were able to fend it off with little disruption.

North Korea’s cyber terrorism is a new challenge on the top of military terrorism that it will focus on developing high techniques with much advanced methodology for effective outcomes. North Korea has been caught in faint with a shocking cyber-offensive that has broad implications for the North’s drive to perfect its ability to deliver weapons of mass destruction to carefully selected targets in Japan, South Korea or possibly the U.S. If North Korean attacks the West or Yellow Sea or possibly across the DMZ between the two Koreas, it can initiate an audacious cyber-offensive over the weekend and revive it to peak levels by mid-week.

Moreover, North Korea recently linked the cyber-offensive directly to a recent flurry of missile tests as well as the test of an underground nuclear device that their security is integrally tied to cyber-warfare. While miniaturizing nuclear warheads to fit on the tips of missiles, part of an effective confrontation with

---


the U.S. war machine could disable U.S. information systems by North Korea’s cyber-terrorism. This strategy fits in integrally with tests of atomic devices in North Korea. North Korea ultimately can stage artillery and missile attacks on major U.S. bases in South Korea in tandem with a full-scale cyber-offensive. The cyber-offensive was enough of a shock to sublimate concerns about North Korean proliferation of weapons ranging from rifles to missiles to components for nuclear devices.

The other hand, South Korean authorities issued a cyber-security warning after the web sites of government agencies and financial institutions were disabled by apparent hacker attacks, possibly linked to North Korea. A series of attacks on computer networks in South Korea and the U.S. was apparently the work of North Korean hackers, several news agencies’ report. The attacks, which targeted the White House, the Pentagon, and the Washington Post, among other high-level institutions, are raising concerns that the long-simmering conflict with North Korea is expanding into a dangerous new theater.¹⁴

Police officers from National Police Agency show a seized computer which was used for hacking at the agency's headquarters in Seoul on July 8, 2009.

According to Seoul’s National Intelligence Service, the attacks appeared to have been elaborately prepared and staged by a certain organization or state. North Korea was not specifically named, but the NIS had traced the attacks to North Korea or pro-Pyongyang forces. Meanwhile, The Associated Press has obtained a list of the targets in a coordinated attack on U.S. networks. Included on the list are the

National Security Agency, the Department of Homeland Security, the State Department, and the Nasdaq stock exchange.

As such, North Korea’s continual cyber attack toward the U.S. is considered as a test of the U.S. government’s ability to deal with a coordinated cyber-attack as data from the U.S. Department of Homeland Security showed that there were some 37,000 cyber attacks in the U.S. in 2007 alone which was going up 800 percent from 2005. The attacks on networks in the U.S. and in South Korea are the latest reminder that cyber-security remains a pressing concern in the 21st century. They may also be a sign that North Korea has stumbled across a new way to provoke its neighbors to the South and its enemies to the West. It also shows that North Korea has put plenty of resources into that technology and that Pyongyang intends on pursuing hostilities on every possible battlefield in this generation of leadership and the next.

4. Future Attacks

Globalization has united the world in variable ways. But it has also made it vulnerable to cross-border crimes at the hands of the terrorists and hackers without having them to cross any border. Now cyber-terrorism turns to be going through everywhere with unlimited attacking skills so that it is unlikely to predict ongoing attacks as well as future attacks. It’s the main concern that what would North Korea’s hackers strike next? A 2006 report by the South Korean military warned North Korean hackers could even paralyze the command post of the U.S. Pacific Command and damage computer systems on the U.S. mainland. The Pentagon adopted a strategy that will classify major cyber attacks as acts of war. The Pentagon plans to release its first-ever strategy regarding cyber warfare as a warning to enemies that try to sabotage the nation's electricity grid, subways or pipelines.

Like North Korea, it is difficult to predict the future direction of politically motivated cyber crime that traditional terrorist organizations will be more involved in cyber attacks. The IRA, Colombian-based FARC and the Red Army Faction all showed some interest in computer hacking but for whatever reason have never carried out any significant attacks. Al-Qaeda supporters operate an estimated 6,000 websites to recruit, proselytize, communicate and plan attacks, but there has been no indication that they plan

---

offensive cyber attacks. Traditional terrorist organizations tend to see the fear and disruption of physical
destruction and death as more effective and easier than a cyber attack. However, as the past two decades
and the increase in recent activity shows, there are a wide range of individuals, groups and possibly
governments that do see network attacks as a means to further their goals and agendas. While we can't
predict the exact targets or impacts of future activity, it is certain that politically motive cyber attacks will
continue to increase and more directly impact our daily lives.\textsuperscript{17} For example, In April 2011, a computer
virus attacked 10 servers of South Korea’s agricultural cooperative known as Nonghyup, affecting 30
million users. They could not use ATMs and online services.

Nonetheless, a recent cyber attack on the South Korea government websites that compromised
classified documents shows the skill of the adversaries we face in the cyber realm. The event, allegedly
carried out by the North Korean army’s elite hacker unit, went all but unnoticed by the vast majority of
cyber stakeholders. It is one of several recent cyberattacks of importance attributed to North Korea.\textsuperscript{18}
North Korea now appears to be fully connected to the Internet. That country is rated among the top 10 in
cyber capabilities and among the top five in cyber ambitions. About 1,024 IP addresses reserved for
North Korea are active, and social networking site feeds operate from locations outside the country on
China’s national Internet. In fact, estimates of the size of North Korea’s hacker force vary wildly an
indication of the poor quality of the data and reports on its cyber capabilities are also complicated by an
imprecise use of terms. Discussions of cyber conflicts usually referred to as cyber attacks, cyber terror, or
cyber warfare often have a kind of breathless, apocalyptic quality about them. But in this case, North
Korea tends to disguise that it could not qualified as a cyber attack, cyber war, or as an act of cyber
terrorism.\textsuperscript{19}

The primary motives for nations to develop cyber capabilities are to prepare for conventional warfare
and to conduct espionage. Like other military powers, North Korea will want the ability to accompany
conventional military action with cyber strikes. For instance, cyber warfare is an important part of

\textsuperscript{17} Kent Anderson, \textit{Virtual hostage: Cyber terrorism and politically motivated computer crime are a big
\textsuperscript{18} Kevin Coleman, \textit{Is North Korea poised to revolutionize cyber warfare.} Defense Systems. Nov 15, 2010. Refer
\textsuperscript{19} James A. Lewis, \textit{Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace.} US-Korea
China’s military doctrine, particularly for use against the U.S. and North Korea has likely studied and perhaps copied it. Absent armed conflict, however, North Korea will likely use cyber capabilities to penetrate the networks of potential opponents to conduct espionage. It is best not to think of cyber-espionage in isolation, however, and instead to consider how North Korea would use cyber techniques to reinforce its already extensive spying by human agents and signals intelligence program.

III. U.S. Cyber-Terror Strategy

It will be the right time to establish an interservice Cyber Warfare Command to coordinate computer defense. Patriotic hackers could be recruited and trained by the military to defend the nation's computer networks from attack. Websites that are damaging to national security, such as Wikileaks, could be attacked if necessary. In certain cases, Special Forces or CIA agents might be used to attack cyber attackers physically.

Since 9.11 Terror, the U.S. has striven to defeat terrorism. But in the end of the Afghanistan and the Iraq War, the U.S. would encountered another security challenge by cyber-terrorism that it is more dangerous in depth and width to disable U.S. military system itself through cyber warfare. The next war that the U.S. should be preparing may be fought in cyberspace on the nebulous electronic territory. In 2005, the Air Force added Cyberspace to Air and Space as its war fighting domains and in 2006, the military authorized a Cyber Command to be temporarily located at the Barksdale Air Force Base in Louisiana.20 At the end of September, 2007, Air Force Secretary Michael Wynne announced that Major General William Lord would direct the Command. Lord has been serving as the director of Cyberspace Transformation and Strategy at the Pentagon since April, 2007. Preparing for potential cyber terrorism attacks will unquestionably be part of its mandate.

The Pentagon has laid out its most explicit cyberwarfare policy to date, stating that if directed by the president, it will launch offensive cyber operations in response to hostile acts. Those hostile acts may include significant cyber attacks directed against the U.S. economy, government or military, Defense Department officials stated in a long-overdue report to Congress released late Monday.21 But the report,

obtained by The Washington Post, is still silent on a number of important issues, such as rules of engagement outside designated battle zones a sign of how challenging the policy debate is in the newest and most complex realm of warfare. The statements are consistent with preexisting policy, but have never before been stated quite so explicitly, even in the Pentagon’s recently released cyberspace strategy.

That strategy focused on the importance of deterring attacks by building defenses that would deny adversaries the benefits of success. In the latest report, the Pentagon states that adversaries threatening a crippling cyber attack against the U.S. would be taking a grave risk. Indeed, officials noted that when defense-based deterrence fails to stop a hostile act, the Pentagon maintains, and is further developing, the ability to respond militarily in cyberspace and in other domains.

1. Government Tactics

RAND Corporation became the latest independent research firm to implore government and law enforcement agencies as well as private-sector IT firms to step up their efforts and get serious about developing a comprehensive battle plan for fighting cyber terrorism in the U.S. and around the globe. The U.S. government as well as corporations seriously start to take a look at cyber warfare. Cyber attacks are even considered as conventional terror attacks with the same importance. For instance, even though they do not rack up the body count of a car bomb or crashing airplane, they have the capability to inflict much more widespread damage on the country as a whole.

It will be the time to establish an interservice Cyber Warfare Command to coordinate computer defense. Patriotic hackers could be recruited and trained by the military to defend the nation’s computer networks from attack. Websites that are damaging to national security such as Wikileaks, could be attacked if necessary. In certain cases, Special Forces or CIA agents might be exploited to attack cyber attackers physically so that cyber agendas will go through new information strategy to fight with. As such, computers and the internet are a vital part of the U.S. economy. We cannot stand idly by while they are attacked by other nations or cyberterrorist groups. Neither should we stand idly by while classified

---


documents that can endanger our soldiers and our allies are released to the world.

The next war that the U.S. should be preparing may be fought in cyberspace on the nebulous electronic territory. In 2005, the Air Force added Cyberspace to Air and Space as its war fighting domains and in 2006, the military authorized a Cyber Command to be temporarily located at the Barksdale Air Force Base in Louisiana. At the end of September, 2007, Air Force Secretary Michael Wynne announced that Major General William Lord would direct the Command. Lord has been serving as the director of Cyberspace Transformation and Strategy at the Pentagon since April, 2007. Preparing for potential cyber terrorism attacks will unquestionably be part of its mandate.

The Pentagon hammered its new cyber policy by revealing a large, previously secret electronic attack on a U.S. defense contractor. In a single intrusion on March, 2011 24,000 files were taken, Deputy Defense Secretary William Lynn said at the release of an unclassified version of the new strategy to defend the U.S. military networks and critical national infrastructure. It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies, adding that the March attack as the latest in a series of escalating attacks over the past five or six years. This digital thievery is interested in the most advanced weapons in the U.S. arsenal. Cyber exploitation being perpetrated against the defense industry cuts across a wide swath of crucial military hardware, extending from missile tracking systems and satellite navigation devices to UAVs (Unmanned aerial vehicles) and the Joint Strike Fighter.

The Pentagon carefully emphasized the defensive parts of its new strategy. Its first goal is to prevent war. But the new plan also makes clear that, if necessary, the U.S. will fight back. The U.S. is prepared to defend itself. Just as our military organizes to defend against hostile acts from land, air and sea, the U.S. must also be prepared to respond to hostile acts in cyberspace, he said. And that response could include what he called a proportional and justified military response at the time and place of our choosing. A central challenge is to identify if and when a cyber attack would constitute an act of war, to prompt military action. An act of war, at the end of the day, is in the eyes of the beholder, Joint Chiefs Vice Chairman, General James Cartwright said at the same rollout of the cyber strategy.

____________________________

In addition to reliance on civilian power, communications and other critical civilian infrastructure networks, the Pentagon has a huge amount of electronic gear to protect - 15,000 networks, and 7 million computers around the world. The WikiLeaks release of hundreds of thousands of military and diplomatic cables dramatically illustrated the inside-job vulnerability of Defense Department computers. And federal officials say that in 2008 a foreign intelligence agency penetrated its classified computer system. Both Cartwright and Lynn stressed that there still is catching up to do as new technology and new vulnerabilities require new legislation and regulation. And Lynn warned that threats will only worsen and become more sophisticated as rogue states and terrorists gain new cyber tools.

The Interpol, with its 178 member countries, is also fighting against cyber terrorism. They are helping all the member countries and training their personnel. The Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, is the result of 4 years work by experts from the 45 member and non-member countries including Japan, USA, and Canada. This treaty has already enforced after its ratification by Lithuania on 21st of March 2004. The Association of South East Asia Nations (ASEAN) has set plans for sharing information on computer security. They were going to create a regional cyber-crime unit by the year 2005.  

Former Defense Secretary Robert M. Gates addresses an audience during the activation ceremony of U.S. Cyber Command at Fort Meade, Maryland, May 21, 2010.

---

U.S. Sailors assigned to Navy Cyber Defense Operations Command (NCDOC) man their stations at Joint Expeditionary Base Little Creek-Fort Story, Va. NCDOC Sailors monitor, analyze, detect, and respond to unauthorized activity within U.S. Navy information systems and computer networks.

Table 2  The U.S. Cybersecurity Strategy

<table>
<thead>
<tr>
<th>Strategic Initiative</th>
<th>Strategy</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Treat cyberspace as an operational domain</td>
<td>Organize, train, and equip DoD can take full advantage of cyberspace’s potential</td>
</tr>
<tr>
<td>Step 2</td>
<td>Employ new defense operating concepts</td>
<td>Protect DoD networks and systems</td>
</tr>
<tr>
<td>Step 3</td>
<td>Partner with other U.S. government departments and agencies and the private sector</td>
<td>Enable a whole-of-government cybersecurity</td>
</tr>
<tr>
<td>Step 4</td>
<td>Build robust relationships with U.S. allies and international partners</td>
<td>Strengthen collective cybersecurity</td>
</tr>
<tr>
<td>Step 5</td>
<td>Leverage the nation’s ingenuity</td>
<td>Encourage an exceptional cyber workforce and rapid technological innovation</td>
</tr>
</tbody>
</table>

Along with the rest of the U.S. government, the Department of Defense (DoD) depends on cyberspace to function. It is difficult to overstate this reliance; DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DoD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations.

The Department and the nation have vulnerabilities in cyberspace. Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity the security of the technologies that we use each day. Moreover, the continuing growth of networked systems, devices, and platforms means that cyberspace is embedded into an increasing number of capabilities upon which DoD relies to complete its mission. Today, many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD’s information infrastructure. Moreover, non-state actors increasingly threaten to penetrate and disrupt DoD networks and systems.  

---

As the Legislative activity, the Cyber Security Research and Development Act (P.L. 107-305),\textsuperscript{28} authorized $903 million over five years for new research and training programs by the National Science Foundation and NIST to prevent and respond to terrorist attacks on private and government computers. The House Science Committee also held a hearing on May 14, 2003 on Cyber security Research and Development, with testimony by the DHS Under Secretary for Science and Technology. A $5 million budget allocation is currently set aside for Information Technology R&D. The Subcommittee on Cyber security, Science, and Research & Development of the House Select Committee on Homeland Security also held a series of hearings on cyber security issues during the summer of 2003.

The series was intended to (1) raise awareness among members of Congress about cyber security risks, (2) examine the views of security experts on the state of security for the critical infrastructure, (3) present the views of industry experts on how DHS might best help resolve cyber security issues, and (4) provide an opportunity for DHS officials to respond to questions raised in the preceding three hearings. On October 1, 2003, the Subcommittee also held an executive session oversight hearing titled, Security of Industrial Control Systems in Nation's Critical Infrastructure with testimony provided by government agencies and by experts on industrial computer systems. Following the September 11, 2001 attacks, the Federal Information Security Management Act (FISMA) of 2002 was enacted giving responsibility for setting security standards for civilian federal agency computer systems to the Office of Management and Budget (OMB).\textsuperscript{80} Responsibility for security standards for national defense systems remains primarily with DOD and NSA.

The following bills identify recent legislative activity that is related to prevention of cyber terrorism, or related to collection of information on possible terrorist activities.

1. \textbf{S. 6} -proposes that information about vulnerabilities and threats to the critical infrastructure that is furnished voluntarily to the DHS shall not be made available either to the public or other federal agencies under the Freedom of Information Act. This bill was referred to Committee on the Judiciary on January 7, 2003. CRS-25

2. \textbf{S. 187} -proposes to eliminate IT vulnerabilities in the federal government to protect against cyber attacks and possible cyber terror. The National Cyber Security Leadership Act of 2003 will require the Chief Information Officer of each Federal agency to report annually to the Director of OMB to: (1)

identify the significant vulnerabilities of the information technology of such agency; (2) establish performance goals for eliminating such vulnerabilities; (3) procure or develop tools to identify and eliminate those vulnerabilities in order to achieve such performance goals; (4) train personnel in the utilization of those tools; (5) test the agency's IT to determine the extent of its compliance with the performance goals; and (6) develop and implement a plan to eliminate significant vulnerabilities in order to achieve compliance. The bill was referred to the Committee on Government Affairs on January 16, 2003.

2. Military Strategy

The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force. Defining cyber battlefield may result in redefining war. Unfazed by taking the fight to the metaphorical domain, the U.S. military has been systematically shaping a strategy to define and arm itself in cyberspace in the new millennium, beginning with the late 1990s concept of 'transformation' to a network-centric military, elaborated in publications such as the 2003 National Strategy to Secure Cyberspace and continuing in periodic doctrinal guides such as the Quadrennial Defense Review. In 2006, the Department of Defense issued a National Military Strategy for Cyberspace Operations which remains classified and committed to the creation of the new Cyber Command. What cyber warfare means and where it occurs is being defined along the way.

According to Lt Col David T. Fahrenkrug, cyberspace is a very real, physical domain that is comprised of electronics and networked systems that use electromagnetic energy. It is not the information that is housed on those systems. It may also be a revolutionary one, because it involves recognizing that cyber warfare differs in one major basic way from traditional warfare because it is not violent. Convertino, DeMattei and Knierim offer up the provocative possibility that cyber warfare may shift fundamentally what we think force, its threat, and war. The ability to fly and fight effectively in cyberspace hinges directly on the proper definition, scope, conceptualization, and integration of tasks, effects, conditions, and objectives of fighting in cyberspace. The military problem of fighting in that realm is new in that it fundamentally involves a nonkinetic, nonviolent approach to war. Cyber capabilities can assuredly

support applications of other orce capabilities, but, fundamentally, they are not the destructive, kinetic purveyors of violence that war fighters traditionally envision in planning military strategy, engagements and wars. If we apply them as primary weapons of war, then basic concepts regarding the use of force or threat of force to compel the enemy must change.

Other cyber security measures include as below.30

<table>
<thead>
<tr>
<th>Division</th>
<th>Cyber Security Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Recognizing that network systems, like everything else, will eventually fail. Therefore, they should be constructed with redundant capability.</td>
</tr>
<tr>
<td>Strategy</td>
<td>Educating managers and CIOs, as well as tech developers, support staff and others, on computing vulnerability.</td>
</tr>
<tr>
<td>Outcome</td>
<td>Making sure that the security tools used are properly maintained. In other words, it is not enough to merely install anti-viral software. One has to be sure to download the updates when they come out.</td>
</tr>
</tbody>
</table>

The Pentagon's first formal cyber strategy represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military. In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. The War on Cyber Attacks is the move to formalize the Pentagon's thinking was borne of the military's realization the U.S. has been slow to build up defenses against these kinds of attacks, even as civilian and military infrastructure has grown more dependent on the Internet. The military established a new command last year, headed by the director of the National Security Agency, to consolidate military network security and attack efforts.31

Since the early 1990s, the U.S. Department of Defense has been worried about the threat posed to its myriad computer systems by malicious outside intrusion. Since 1995, DoD systems have been regularly attacked, up to 250,000 times a year, and only about one of every 50 attacks is detected and reported. This primer lays out the progress of the Defense Department’s response to the threat to its information

networks. The Defense Department established its first unit to combat cyber threats in 1998. The primary motivation for the establishment of the initial unit, then known as Joint Task Force-Computer Network Defense, in late 1998, was a series of exercises and real events that demonstrated to DoD that a fresh approach to the problem was necessary. Two principal factors were: Exercise Eligible Receiver 97, in which National Security Agency (NSA) personnel inflicted, in simulation, a large amount of damage upon defense networks; and, a computer hacking attack at first feared to be the work of Iraqi agents during a confrontation with Iraq in the Middle East in late 1998. Exercises such as U.S. Atlantic Command’s Evident Surprise also contributed to the increasing awareness of many systems’ vulnerability.

Directed by the chairman of the Joint Chiefs of Staff and run from June 9-13, 1997, Eligible Receiver 97 was the first large-scale, no-warning military field exercise crafted to test the ability of the United States to respond to an attack on both U.S. military and civilian information infrastructure. The exercise involved simulated attacks against components of the civilian infrastructure, such as power and communications companies, and an actual "opposing force" attack against key defense information systems at the Pentagon, the Joint Staff, the Defense and Central Intelligence Agencies, other supporting agencies, and in the unified combatant commands. The vulnerabilities exploited were common ones, such as bad or easily guessed passwords, operating system deficiencies, improper system configuration control, inadequate user awareness of operational security, sensitive site-related details posted on publicly accessible Internet pages, and poor operator training. The opposing force team, drawn from the National Security Agency (NSA), was given no inside information, but was still able to inflict considerable simulated damage partially due to its extensive preliminary electronic reconnoiter of target agencies and sites prior to the attacks.

Several months later, from Feb. 1-26, 1998, a number of computer attacks were detected that appeared to be originating from, amongst other places, the Middle East. At least 11 attacks were launched on a number of Navy, Marine Corps, and Air Force computers worldwide, primarily focusing on denial of service. The attacks exploited a well-known vulnerability in the Solaris operating system, for which a patch had been available for months at the time. As the attacks were launched as the U.S. military were preparing for possible combat missions against Iraq, there was much concern, and an interagency investigation, named ‘Solar Sunrise,’ was initiated. The Air Force, Navy, Army, NASA, the NSA, the Department of Justice, the CIA and FBI were all involved in the investigation. Given the circumstances, numerous court orders were issued quickly and it was found that the culprits were two California
teenagers and an 18-year old Israeli mentor. Despite the fact that none of the systems involved were classified, the security breaches could have been used to disrupt DoD information flow in a possible Middle East war, and consequently, the investigation was one of the largest ever conducted in the U.S.

Due to the high prominence of the ‘Solar Sunrise’ attacks and the previous experience during Eligible Receiver 97, the Defense Department moved relatively quickly to take a number of defensive measures. They included: - Increasing situational awareness via a 24-hour watch center. Installing intrusion detection systems on key systems nodes. - Expanded computer emergency response teams to perform alerts, critical triage, and repair. Developing contingency plans to mitigate the degradation or loss of networks. - Improving DoD’s ability to analyze data rapidly and assess attacks. Improving links with the FBI’s National Infrastructure Protection Center and other law enforcement agencies.

The operational response issue was specifically addressed by the formation of the Joint Task Force-Computer Network Defense (JTF-CND), activated on Dec. 30, 1998. After six months, it achieved full operational capability in June 1999. JTF-CND was assigned to U.S. Space Command in October 1999 as Space Command was assuming the Pentagon’s computer network defense mission. The JTF-CND is located in Arlington, Va., alongside the Defense Information Systems Agency’s Global Network Operations and Security Center. It incorporates the DoD’s Computer Emergency Response Team (CERT), and the four service Computer Emergency Response Teams. Three of the four CERTs are stationed in the Washington area. The original nucleus of the JTF-CND consisted of approximately 40 uniformed and civilian personnel including intelligence specialists, DoD law enforcement personnel, and counter-intelligence special agents focusing on computer-related criminal activity. Mid-2001 congressional testimony indicated that the JTF-CND is now set to grow to about 144 personnel.

A year after the JTF-CND was assigned to Space Command, Space Command gained the computer network attack offensive information warfare - mission; and, on April 2, 2001, the unit was re-designated the Joint Task Force Computer Network Operations to reflect the fact that it was to perform that mission as well. More importantly for its cyber-defense mission, the revised unit has embarked on building relations with other involved agencies, such as the National Infrastructure Protection Center (which is now proposed to become part of the Homeland Security Department); and, the National Communications System, a confederation of 22 federal agencies and departments tasked with ensuring the availability of a safe and viable telecommunications infrastructure. Indeed, the Joint Task Force’s defense computer security mission will rest to some extent on the linkages it establishes with other government agencies and private companies facing the same situation.
The Defense Department continues to be faced with computer infiltration difficulties beyond the scope of routine computer viruses and relatively unsophisticated hacker attacks. Most publicized was an apparent incursion from Russia in 1999, whose investigation codename was Moonlight Maze. It seemed to originate from the Russian Academy of Sciences. This attack, in concert with others, helped spur the development of automated intrusion detection systems, which have made a huge difference in DoD’s ability to detect and respond to cyber incursions. Further advanced work is now in progress within the NSA to identify an intruder even before he/she enters a DoD system. Much of today’s problems - there were 14,500 attacks in 2001, of which 70 made it into DoD computers and three caused damage - result because system administrators who do not install routine patches. The three attacks that caused problems in 2001 were the same as those that damaged private computer networks at the same time. While DoD seems to be making progress in its cyber defenses, much work remains to be done to educate users and systems administrators alike, as well as stay ahead of the ever-creative hackers.

The U.S. military must shift its focus to fighting a wide range of threats from cyber attacks to terrorism as the Pentagon's 2010 draft strategy. It revises the previous objective of being equipped to fight two major conflicts at any time. The strategy accounts for threats such as cyber attacks, global warming and "hybrid" guerrilla-style insurgencies. It comes on the same day that the U.S. defense secretary unveils his budget. Robert Gates' proposed 2011 spending plan comes to more than $700bn (£440bn), a modest 2% increase, the draft documents show. But it avoids the sweeping cuts to major weapons programmes seen in last year's budget. The Pentagon is mandated by Congress to review America's defense priorities every four years.

IV. U.S. Cyber Strategy toward North Korea’s Cyber Terrorism

The New Pentagon Strategy emphasized that the U.S. shift in focus to Asia comes amid increasing concern at the Pentagon over China's strategic goals as it begins to field a new generation of weapons that are designed to prevent U.S. naval and air forces from projecting power into the Far East. As strengthening the U.S. presence in the Asia-Pacific, the new strategy calls for the U.S. military to "rebalance toward the Asia-Pacific region" even as it continues to actively counter the threat of violent extremism. It also calls for increased investment in cyber capabilities and suggests the U.S. may be able

to shrink its nuclear arsenal further without jeopardizing security.33

According to the draft 2010 quadrennial defense review: It is no longer appropriate to speak of 'major regional conflicts' as the sole or even the primary template for sizing, shaping and evaluating US forces. It highlights "a multiplicity of threats", including satellite and cyber attacks, as well as terrorist groups and the prospect of more nuclear-armed nations. The plan allocates new funding for helicopters, unmanned planes and special operations units, which have played a key role in both conflicts. It outlines a joint Air Force-Navy battle plan to counter the threats from nations such as China, Iran and North Korea, citing their increasingly sophisticated aerial defense and strike systems. The report says Mr Gates will also seek to overhaul the military's acquisitions system so the US can get key supplies quickly to its own bases and those of its partners around the world. The review for the first time identifies global warming as a potential trigger of instability or conflict around the world.

Therefore, when does a cyber attack by another nation cross the line and become an official act of war?34 Government and private company Web sites in the U.S. and South Korea were attacked by unidentified hackers who tried to crash them. Target institutions in the U.S. included the departments of Transportation, State and Treasury, the White House (reportedly), the New York Stock Exchange, Yahoo and the Federal Trade Commission. In this case, the vehicle appears to have been a well-known software "worm" that was reprogrammed -- and not particularly well, it seems -- for the task. Still, for all of its crudeness, the attack did work. In the U.S., some sites were down for as much as 24 hours. In South Korea, some remained crashed Thursday.

North Korea’s cyber terrorism will be beat up by the U.S. cyber strategy whenever it is taced as North Korea’s bold attacks. North Korea’s cyber terrorism will be terminated that the U.S. sets up cyber strategy not to allow North Korea’s threat. Like nuclear weapons, North Korea’s cyber terrorism will induce its collapse and end up its sovereignty sooner or better. However, North Korea’s cyber terrorism will work out the turning point that the U.S. focuses on upgrading more advance militaty techniques over the traditional military power on the cyberspace to win cyber war as only the military super power to dominate the international society.

References


