# World War III

## A Cyber War has begun

*September 2007*

**INTEL:** Moonlight Maze is the U.S. government's code name for a series of coordinated attacks on U.S. computer systems in 1999. This was a two year attack that was discovered by the Department of Defense. The attacks were traced back to a main frame computer in Moscow but it is unclear at this point if that is where they originated or who was behind the incidents. A high placed source stated this is still an open and active investigation today. Titan Rain was the U.S. Government's code name for an ongoing series of cyber attacks on U.S. computer systems since 2003. Titan Rain is thought to rank among the most pervasive cyber security threats that U.S. computer networks have ever faced. At this time investigators believe that this is a coordinated attack involving about two dozen hackers. Just recently, the "Titan Rain" code name has been changed, and the new name for the attacks is classified.

The Technolytics Institute
4017 Washington Road
Mail Stop 348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193
I www.technolytics.com

technolytics


Recently a series of cyber attacks on the Defense Department and Defense contractors in the United States as well as the Ministry of Defense and Parliament in the U.K. have created significant cause-for-concern by computer security experts. An investigation of the attack signatures shows a significant level of sophistication. Most are "highly skilled professionals" said one source who wished not to be identified. The most recent cyber attacks are using new strains of computer viruses, logical bombs and other advanced techniques that can paralyze government agencies and communications. Information for exploiting known computer vulnerabilities is easily obtainable by anyone via the Internet. Programs covering nearly every aspect of hacking, from Trojans to keyloggers to step-by-step tutorials on how to effectively hack computer systems, are now available on eBay's online auction site. Individuals do not need to be overly technical to use these hacking tools either. Making a much broader audience aware of how easy it is to get these tools and use them has security professionals concerned. One computer insider said that there is evidence that a criminal enterprise has been established whose sole purpose is to create hacker kits to exploit software vulnerabilities as soon as they are publicly disclosed. One such hacker kit developed last year sold for over $50,000 per copy. This is big business.

### Cyber Warfare Arsenal

At this time intelligence sources are unsure the number of countries developing or acquiring cyber weapons nor the size and capabilities of their cyber arsenals. Many questions remain unanswered.

Insiders have said that the full extent of the U.S. cyber-arsenal is among the most tightly held national security secrets, even more guarded than nuclear capabilities. However, since last year there has been a 46 percent increase in attacks on Department of Defense web sites. In the response to the threat posed by the widely available arsenal of cyber weapons, the U.S. Navy increased its cyber defense force from 200 sailors to 15,000 in the past three years? The navy is now spending nearly a billion dollars a year to defend its computer systems.

- Computer worms
- Software vulnerability exploitation
- Denial of service attacks
- Info-blockades
- Root kits
- Botnets
- Malicious code
- Keyloggers
- IP spoofing
- Logic bombs
- Sniffing
- Spamming
- Trap doors
- Trojan horses
- Video morphing
- Viruses

## ESTONIA ATTACKED

In April of this year Estonia was the target of a coordinated attack on their national internet infrastructure which all but crippled the country. The attack lasted about three weeks and involved an estimated 1 million computers. The massive denial-of-service (DOS) attack was thought to be launched by Russian hackers. The attacks on Estonia began April 27. The attack used "botnets" (swarms of computers hijacked by malicious code) to overload sites and networks by deluging them with bogus requests for information. Estonia has a population of about 1.3 million and is one of the most wired countries on earth. The intent of the attack was to shut down the country's information infrastructure. This impacted Estonia's citizens' ability to execute financial transactions as well as impacting the country's supply chain for food and other products. For example, at the peak of the attack, people who wanted to use payment cards to buy bread or gas had to wait because the traffic overload created by the attack all but halted operations at Estonia's banks.

In the book "Unrestricted Warfare" published back in February of 1999 it suggests tactics that can be used by developing countries (like China) to overcome military inferiority when going up against countries like the United States. This concept has continued to evolve and now consists of fifteen different modalities of warfare employed against an enemy.

*Note: For additional information on the concept of UnRestricted Warfare, please refer to Eye Spy Magazine Volume Number 40 published in 2006.*

Global Leaders face a new threat environment unlike any we have previously experienced in the past. Our offensive and defensive capabilities must be built to address the full spectrum of warfare in the 21st century. Earlier this year an article in the Washington Post reported President Bush has signed a secret directive ordering the government to develop a national-level policy for determining when and how the United States would launch cyber-attacks against enemy computer networks. The Department of Homeland Security created the National Cyber Security Division (NCSD) under the Department's Information Analysis and Infrastructure Protection Directorate. The NCSD conducts cyber attack analysis and improved information sharing, across a number of organizations involved in protecting and securing the information infrastructure. This was part of the National Strategy to Secure Cyberspace and the Homeland Security Act of 2002. Just recently, the Department of Homeland Security (DHS) and the National Security Agency (NSA) have joined forces and launched a massive cyber initiative with some 2,000 analysts. Sources have stated that this coordinated effort is directly related to the recent escalation of cyber attacks. Additionally, the National Security Agency and U.S. Strategic Command (StratCom) personnel have been working together developing enhanced cyber weapons that have the ability to attack and exploit foreign computer networks. It appears that every branch of the United States military are developing their own cyber attack capabilities.

Attacks on telecommunications systems and computer networks have been called the invisible threat to the national economy and security. Day after day, digital warriors defend our information systems and infrastructure against thousands of unseen attacks by criminals, enemy states and terrorists. In analysis provided by Spy-Ops, nearly 3.9 million computer attacks have been reported in the last 24 hours. This clearly shows the magnitude of the problem.

**INTEL**: In the past four months, Chinese hackers have allegedly targeted German, the United States, and French, UK and other NATO organizations information systems and infrastructure.

**INTEL:** Cyber conflicts are often referred to as the silent war.

**INTEL:** In August of 2007, Chinese hackers installed Trojan horse programs on many PCs in the German government and related organizations using booby-trapped Microsoft Word files (.DOC) and Microsoft PowerPoint files (.PPT), according to sources close the investigation in Germany. China is already a world power and will soon be a superpower challenging the U.S. and Europe.

**INTEL:** The Cyber War that has been raging against the United States and other has gotten a lot worse. Now top Government Officials are paying more attention. On September 29th, 2007 a top team from the NSA (National Security Agency) has been called in to play a major role in defending civilian U.S. networks from attacks coming in via the Internet

## MEASURING THE THREAT

The following cyber threat matrix has been developed by Technolytics with support from Intelomics and Spy-Ops. It examines the intent and capabilities of six potential enemy nations as of mid 2007.

# CYBER THREAT MATRIX

| Country | Estimated Military Spending | Intent | Estimated Threat | Current Capabilities | Basic Data Weapons | Intermediate Data Weapons | Advanced Data Weapons |
|---|---|---|---|---|---|---|---|
| China | $55.90 | 5.0 | High | 4.2 | Yes | Yes | Yes |
| Iran | $9.70 | 4.0 | Elevated | 3.4 | Yes | Limited | No |
| Libya | $1.30 | 3.0 | Moderate | 2.5 | Yes | No | No |
| North Korea | $5.20 | 3.0 | Elevated | 2.8 | Yes | Limited | No |
| Russia | $44.30 | 5.0 | High | 4.0 | Yes | Yes | Yes |
| Syria | $8.90 | 3.0 | Moderate | 2.2 | Yes | No | No |

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

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

No one (military or private sector) should assume that adversaries lack the sophistication to take advantage of software vulnerabilities. Nor should they turn a blind eye to the fact that more and more equipment like cell phones, automobiles and other devices have microprocessors and software built into them and connect the internet. The exposure to cyber attacks grows with every new device that connects to the internet or our internal networks.

It is also important to realize that individuals can pose as much of a threat as rogue nation states. A British man hacked into nearly 100 computer networks operated by the military and NASA. For over a year the man stole passwords, deleted files, monitored traffic and shut down computer networks on military bases from Pearl Harbor to Connecticut and 2 of the computer break-ins were at the Pentagon. An army of one can cause significant damage and disruption to computer systems and networks.

A U.S. Defense Department report indicated that China's blueprint of cyber war is part of a plan to dominate the cyber world surpassing its competitors like the U.S., the U.K., Russia and Korea by 2050. This is a clear indication of the growing threat of cyber warfare. One report charges that China has been engaged in cyber theft and attack against the U.S. and other countries that it perceives as its enemies for years. In 2005, security analysts tracked a series of cyber assaults against U.S. computers, code named Titan Rain, to 20 computer workstations in China's Guangdong province

During a September 4th press conference, Jiang Yu , a Chinese Foreign Ministry Spokesperson, said "Some people make wild accusations against China." Beijing has denied any involvement in the cyber attacks, and the Western governments have been unwilling to publicize exactly what, if any, evidence they have and if any classified information was compromised.

**FACT:** China is rising rapidly as an Asian political and economic power and is modernizing its army to fight and win short-duration, high-intensity conflicts along its borders, according to a new Defense Department report.

**Fact:** China is second to only the United States in military spending. They recognize the lead the United States has on them in the area of $C^4ISR$ (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) and wants to disrupt or even remove that advantage.

## MEASURING THE THREAT

Most countries are complacent with regard to protecting their information infrastructure. A U.S. Congressional Committee on computer security has given failing grades to many of the federal organizations it scrutinizes. The following cyber defense matrix has been developed by Technolytics with support from Intelomics and Spy-Ops. It examines the defense capabilities of six nations as of mid 2007.

INTELOMICS
SUPERIOR INTELLIGENCE THROUGH TECHNOLOGY

## CYBER DEFENSE MATRIX

| Country | Technical Capabilities | Defense Commitment | Defense Capabilities | Current Capabilities | Basic Defenses | Intermediate Defenses | Advanced Defenses |
|---|---|---|---|---|---|---|---|
| U.S. | 4.2 | 4.5 | High | 4.2 | Yes | Yes | Yes |
| U.K. | 4.0 | 4.1 | Elevated | 3.7 | Yes | Yes | Limited |
| Russia | 3.7 | 3.2 | Moderate | 3.8 | Yes | Limited | Limited |
| Syria | 3.2 | 2.8 | Moderate | 2.8 | Yes | Limited | No |
| Israel | 3.5 | 4.2 | Moderate | 3.9 | Yes | Yes | Limited |
| Iran | 3.8 | 4.5 | Moderate | 3.7 | Yes | Limited | No |

*Estimated Military Capacity to Defend Against Cyberwarfare*

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

Most defenses against cyber attacks are very rudimentary and reactive for two main reasons. First, public – private partnership is required in order to implement many of the defenses and that is always a difficult obstacle to overcome. The second reason is that much of the computer manufacturing and software development is done offshore. I was on a science and technology advisory committee and in one case we looked at nearly 85% of the systems related equipment was sourced outside the United States. Foreign influence in the computer and information technology sectors is high and growing.

In 2004, then Defense Secretary Donald Rumsfeld approved a newly drafted Infocentric Operations Roadmap that is said to outline the capabilities being developed for offensive cyberwarfare. The Roadmap "represents 18 months of effort to determine Infocentric Operational issues and made 57 recommendations for implementation. Execution of these 57 recommendations is already well underway, In November of 2006, the U.S. Air Force set up a new cyber warfare group, called the Cyberspace Command and is rapidly developing their strategy and weaponry.

The cost of entry into these emerging weapons of mass disruption is very low. It is important to note that smart people are the key to developing data weapons. A few computers, a network connected to the internet, and people who understand software and systems is all it takes to enter the cyber weapons race. It is important to realize that you cannot tell if an adversary has cyber weapons until they use them!

These threats are real and our defenses are weak. Worst of all, the threat of a Cyber War has all but faded from most people's memory. What would a cyber war be like? Use of scenario planning will help to anticipate the challenges but, with so many ways to be attacked by hackers it is difficult to construct a cyber security strategy and plan.

**INTEL:** In July of 2007, German officials proposed to use of Trojan horse software to secretly monitor potential terror suspects' hard drives, amid fierce debate over whether the measures violate civil liberties.

**INTEL:** The U.S. military launched a cyber attack on Iraq as part of its 2003 invasion. This is thought to be the first use of cyber warfare in conjunction with conventional attacks in history. While there have been numerous cyberskirmishes between attackers in China, Taiwan and the U.S. in the past decade, this was an all out attack.

## Cyber Attack Scenario Planning Exercise

Using Scenario-based Intelligence Analysis (SBIA) and Transdisciplinary Intelligence Engineering (TIE) the following scenario has been rated a likely scenario. A cyber attack requires detailed planning in order to go undetected and achieve the strategic objective. While many believe this is very difficult, the following scenario proves otherwise.

Strategy: Use malicious code hidden inside computer imported by a country

Objective: Mass disruption of a nation's information infrastructure

Weapon: Massive distributed denial of service attack

Plan: Create the capability to launch a massive denial of service attack from within a targeted country. This could be accomplished by inserting malicious code into personal computers and laptops at the point of manufacture.

Tactic: Covertly place malicious code in millions of computers at the point of manufacture. Hiding malicious code into the reported 50 million lines of code in VISTA or the reported 55 million lines of code in Linux would be the mechanism of delivery for the attack.

Imports: The United States imports a significant amount of advanced technology. One report showed that China exported nearly $74 billion of advanced technology products to the United States. In 2006 the following table indicates the top three countries exporting computers, information and communications equipment into the U.S. The percentage represents the imports percentage of the market.

| | | | | | | |
|---|---|---|---|---|---|---|
| Computer software | Mexico | 23.7% | China | 17.0% | Canada | 16.6% |
| Information and communications | China | 40.5% | Malaysia | 13.4% | Mexico | 10.1% |

Cyber Defense Agency, an information security and research company warned in 2006 that widespread use of outsourced commercial software by the U.S. organizations could expose the nation to cyber attacks caused by malicious code buried deep within the millions of lines of software.

Detection: Uncovering this kind of attack with current testing techniques and practices is highly unlikely. It is like looking for a needle in a hay stack – a few lines of code dispersed throughout the millions of legitimate lines of code. Limited tools are available to detect the hidden code so the primary method of detection would be manual code inspection. Given that every computer would have to be checked for the hidden code, the likelihood of detecting this type of an attack would be very, very limited.

Result: At a designated time, all the computers infected with the malicious code would begin to flood the networks they are connected to with malicious transactions. This flood would inhibit the networks' ability to conduct legitimate transactions. As the volume of malicious transactions increase, the associated server(s) and network(s) would fail.

Spy-Ops

Scenario-based Intelligence Analysis (SBIA) is a methodology pioneered by Spy-Ops. In 2006, it was featured in an article in Cyber-Terrorism Magazine which drew the following response.

"Scenario-Based Intelligence Analysis (SBIA) is a force-multiplier, value-added intelligence concept that can yield returns for the decision-maker. Not only can SBIA help reduce ambiguity that often plagues intelligence analysis, it also answers the "So what?" of information collected. In the analytical world, this is where the rubber meets the road."

*David Jimenez, Faculty*
*American Military University*

## An Insider View

An un-named source at Intelomics who is a security and intelligence subject matter expert stated that we are in a new era of conflict. Body-count, bomb damage assessments and other metrics and measures that have been used to report military progress will be of little relevance in the age of cyber warfare. Silent attacks are waged daily that threaten the electronic society we live in. The short-sightedness of governments and businesses has left all of us at significant risk. This is not a problem that will go away anytime soon!

## Conclusion

The threats we currently face represent a new way of thinking about conflict and warfare. Cyber attacks are particularly dangerous because of the world's reliance on computers, networks and technology. These computers control critical systems that run power plants, telecommunications infrastructure, air traffic and more. Cyber attacks on banks, stock markets and other financial institutions could have a devastating economic effect on any country. With international law lagging in the area of cyber crime and cyber warfare, it resembles the early days of the wild-west (untamed territory).

The recent events are clearly cases of state-sponsored governmental and corporate espionage. Spy-Ops estimated that corporate espionage alone has grown to be a $1.5 trillion problem. Countries around the world need to wake up and recognize the danger of cyber warfare. In the spring of 2001 literally weeks after I left Netscape, I testified before members of the U.S. Congress and demonstrated the ease with which one could break into a computer. In the live demonstration over a 56k dial up line, we were able to hack into the computer through a properly configured firewall, with antivirus and all the latest updates. The warning and predicted attacks on the information infrastructure has now become a reality. Significant action must be taken now by the United Nations and individual countries to protect the critical information infrastructure and secure the electronic backbone of society. Developing, equipping and deploying Cyber Warfare units are critical if we are to ensure any countries' survivability, prosperity and stability. Additionally, development of international law that addresses the complex issue of cyber attacks.

In closing remember that for every breach you read about there are at least a dozen others that go unreported. The clock it ticking and the countdown begun. We are only mouse clicks away from a massive cyber attack. Are you ready?

**Fact:** The advances in cyber attack techniques currently being used all over the world have become very sophisticated. This rapid advancement of attack techniques has significantly outpaced improvements in security.

**Fact:** According to computer security experts, about 1,000 new computer viruses are seen every month. Some 250 are completely new and 750 are modified versions of previously discovered viruses.

**Fact:** In 1999 Chinese hackers took down three U.S. government sites after NATO bombers mistakenly attacked the Chinese embassy in Belgrade.

**Fact:** Al Qaeda prisoners interrogated by the United States have admitted to their intention to use cyber weapons to attack the critical infrastructure of the U.S. and others.

# Addressing Strategic Issues
## *of Business, Government and Industry*

An Strategic Approach to . . .

... Security

... Compliance

&

... Risk Management

*The Technolytics Institute*