Table of Contents

CYBER DEFENSE HARDWARE VULNERABILITIES ................................................................. 2

ESCALATION OF CYBER ATTACK ACTIVITY ........................................................................ 2

THE CYBER THREAT ENVIRONMENT ................................................................................. 3

METHODS OF CYBER ATTACK .......................................................................................... 3

HARDWARE VULNERABILITIES ......................................................................................... 4

NATIONAL RESPONSE....................................................................................................... 5

SUMMARY .......................................................................................................................... 8

ENDNOTES .......................................................................................................................... 9

APPENDIX A: CYBER WARFARE TIMELINE: SELECTED EVENTS ...................................... 10

APPENDIX B: NATIONAL CYBER INITIATIVES.................................................................. 19
Cyber Defense Hardware Vulnerabilities

*Escalation of Cyber Attack Activity*

The world is experiencing revolutionary growth in the number of cyber attacks. The last few years have seen a remarkable rise in the rate and sophistication of such activity, which has been carried out against a broad range of target institutions, including groups widely separated from national and political institutions. *The Cyber Warfare Timeline in Appendix A covers a partial list of cyber warfare activity since 1969.*

Efforts by countries to obtain the capability to conduct cyber warfare are escalating globally at an alarming rate. In 2006, there were an estimated 22 countries pursuing cyber weapons. In 2008 that number had raised to approximately 140 countries—some 70% of the nations in the world.¹ It is almost certain that an increasing number of new, more sophisticated strategies will be developed to carry out these attacks. The magnitude of the problem can be illustrated by a single example: In 2008 an estimated 360 million cyber attempts were launched to break into Pentagon computer systems.² Unquestionably a global cyber arms race is underway.

Further, discoveries of counterfeit cyber equipment in the supply chain are becoming more frequent. The increase in counterfeiting indicates a cyber security risk from an emerging and dangerous method of attack.

*In November and December 2007, coordinated U.S. and European customs and border operations confiscated 360,000 counterfeit integrated circuits and other network components imprinted with 40 different trademarks.*³

*In 2005, the Office of Technology Evaluation (OTE) sampled 387 companies in the U.S. supply chain from component manufacturers to prime contractors looking for counterfeit discrete electronics, microcircuits, and circuit boards –key elements of electronic systems. OTE found 3,868 incidents of counterfeit parts being provided for use in sensitive government weapons and communications equipment. When OTE repeated the sampling in 2008, 9,356 incidents were discovered – a compound growth rate of 34.2%. In the more recent sampling, 39% of the companies were found to have counterfeit electronic parts in their supply chain.*⁴
The Cyber Threat Environment

Threats to those operating in the new cyber domain are markedly different from those in other environments, because the environment itself is unlike that of any physical environment in which conflict normally occurs. The land, sea, air, and space domains have similarities in that threats are presented in physical space, come in predictable ways, and can be defended against with sensors and weapon systems. The attacks normally involve weapons that cause physical destruction.

By contrast, the cyber domain is man-made and has several characteristics that make it unique: Attacks occur in milliseconds, often from obscured sources, and can be launched against any integrated system from any other such computer in the world without notice.

Cyber attacks present a formidable challenge; often the best outcome may be only to deny attackers their objective. Frequently it is hard to trace the source of the attack or assign responsibility for it. Hence, perpetrators are likely to operate with anonymity and remain free from capture or prosecution. Unfortunately, another unique feature of cyber warfare is that hostile actions against cyber systems, even ones launched by other nations, are not currently viewed as acts of war. Attacks are generally treated as a form of espionage even though the threats can pose serious risk to national security or a nation’s defense or industrial assets.

Methods of Cyber Attack

Protecting cyber systems involves first identifying vulnerabilities. There are four general paths into a cyber system to steal, corrupt, or control it. The first is human direct input. This involves traditional physical entry such as inserting discs or memory sticks, entering data through keyboards, or using voice commands. Attackers can carry out intentional strikes in which they plan specific damage, or they can be unintentional agents who are unaware of a destructive program hidden on a memory device that they insert into a system. The primary protection from these attacks is physical security and human entry screening security.

Some experts feel the most significant publicly acknowledged cyber security breach in U.S. history occurred at the Pentagon in 2008. Authorities believe the breach occurred when a flash drive left lying in a place where U.S. military personnel were likely to pick it up was inserted and used in a military laptop connected to the CENTCOM computer system. The flash drive had been infected by a foreign intelligence agency.
By using the malicious code loaded onto the flash drive, the infiltrator accessed the CENTCOM network, gaining both unclassified and classified information from the database being used for command of U.S. forces in Iraq and Afghanistan. The invader remained active in the system for several days, able to access documents, monitor communication traffic, and potentially interfere with activities.5

The second path into a cyber system is through another computer that is connected directly to the network on which the cyber system resides. A computer already compromised can be used as a means of attacking a cyber system that might otherwise seem protected from tampering. The best protection against attack from connected computers is coordinated physical protection of all connected systems, or detaching computers containing sensitive information from other systems.

A third type of entry is signal infiltration: this involves the transmission of electronic signals allowing the attacker to gain access or affect systems performance. These kinds of remote attacks, especially ones generated over the Internet, are the easiest and safest forms of assault for any enemy. The growth rate in signal infiltrations globally is alarming, especially since it is particularly hard to defend against this form of attack. Not surprisingly, this problem is getting significant attention from most government and commercial organizations as they develop their defense strategies. It is the issue that dominates the national debate on protection.

A fourth method of attack—one that often requires great sophistication and planning—is to corrupt cyber hardware at the manufacturing point or along the supply chain. This activity could involve counterfeiting or tampering with hardware such as integrated circuits installed on the machines without the user’s knowing that the device or product has been corrupted. **Hardware penetrations are a desirable method of attacking cyber systems because they offer attackers the opportunity to gain control of the invaded system, are exceedingly hard to detect once installed, and can be activated in a fashion similar to that used for sleeper cells in more conventional espionage operations.**

**Hardware Vulnerabilities**

Microelectronics hardware risk has long been acknowledged as a serious problem: Our national defense and critical security systems are dependent upon leading-edge microelectronics that are increasingly produced outside the U.S. without adequate, if any, security processes.

In 2003 DEPSECDEF published the Defense Trusted IC Strategy, that launched a series of initiatives to be undertaken by both Department of Defense (DoD) and the National Security Agency (NSA) to ensure that the defense and intelligence
Communities have ready access to trusted state-of-the-art microelectronics sufficient to meet the needs of mission critical and mission essential systems.

Later that year, the DoD and took positive steps toward solving this problem by establishing the Trusted Foundry Program: an arrangement with the single domestic supplier who was willing and able to provide secure access to leading-edge semiconductor design and manufacturing processes. This program has proven to be adequate for supplying microelectronics to the intelligence community and the research and development (R&D) community in the DoD.

Recognizing that a single, domestic supplier could not satisfy the entire DoD procurement base, the Trusted Foundry Program authorized the Defense Micro Electronics Activity (DMEA) to develop and implement an accreditation process that would engage other U.S. microelectronics suppliers in the program. Today, 46 private facilities or research labs have invested in the process of becoming Trusted Foundry Program accredited suppliers.

The focus of the Trusted Foundry Program has been to assure the microelectronics in defense and national security systems are free from tampering and will perform as needed, when needed. Certainly our national cyber infrastructure deserves the same level of hardware assurance.

Yet despite the $500m investment to build the capacity to provide access to trusted microelectronics, the linkage between hardware vulnerabilities and cyber defense has been largely absent from national initiatives.

Most efforts to protect systems against cyber attacks currently are focused on signal attacks. Nevertheless, compromised hardware or software present an equally dangerous problem. At present, defenses against such attacks are clearly not in place.

**National Response**

The United States Government has been involved in battling global threats to cyber security for decades. At the same time, the Government is probably the most actively targeted organization in the world. To counter cyber threats, several actions have been taken to formalize a cyber defense plan for Government assets. In January 2008, the Bush Administration established the Comprehensive National Cybersecurity Initiative (CNCI) to identify and close security gaps that exist between attacks and defenses. This classified joint Presidential directive was designed to foster development of policy, strategy, and guidelines to secure federal systems. Five months later the DoD announced the formation of a new U.S. Cyber Command (USCYBERCOM) to integrate cyber operations throughout the U.S. military.
Obama administration published an unclassified summary of the CNCI in March of 2010.° (Appendix B contains a list of CNCI initiatives and the URL that provides access to the White House document and greater detail about each initiative.)

The threat to Government systems certainly warrants such a high level response. Deputy Secretary of Defense William Lynn noted in a recent article that the United States has evidence that 100 foreign intelligence organizations are trying to break into the U.S. networks and those of other nations.°° This highlights the existing gap between attack capability and defense capability. The CNCI initiatives outline a plan for defense for the threat being faced by the Government today.

The CNCI lays out a strategy for dealing with specific complexities of the Government’s cyber systems. The DoD reorganization to form a command to coordinate activities aimed at cyber defense is a useful signal to other systems managers that the cyber domain and its threats are best addressed in a unified approach rather than by using a traditional security organization structure. These steps are at the heart of recognizing the unique and dynamic nature of the cyber domain and the particular nature of threats aimed at exploiting, disrupting, or destroying cyber systems, whether government-run or under the control of private enterprise.

Nevertheless, a more comprehensive view of the cyber domain and its future trends is required that acknowledges the hardware vulnerabilities.

“Compromised hardware is, almost literally, a time bomb, because the corruption occurs well before the attack . . . Maliciously tampered integrated circuits cannot be patched . . . They are the ultimate sleeper cell.” General Wesley K. Clark 11

The Trusted Foundry Program provides an established path for cyber security protection at the hardware level. At the heart of mission-critical weapons and command and communications systems are microelectronics components that must function properly and reliably and be free from malicious tampering.

Hardware supply chain tampering threats may portend the most serious cyber security threats as microelectronics may be compromised by tampering or the substitution of counterfeit parts at any point between manufacture and installation.

Today’s cyber security threat warrants a new program that incorporates the Trusted Foundry Program’s assets into a broader hardware-based cyber defense initiative.

The risk of compromise in the manufacturing process is very real and is perhaps the least understood cyber threat. Tampering is almost
impossible to detect and even harder to eradicate. Already, counterfeit hardware has been detected in systems that the Defense Department has procured.

The Pentagon’s Trusted Foundry Program, which certifies parts produced by microelectronics manufacturers, is a good start, but it is not a comprehensive solution to the risks to the department’s technological base. Microsoft and other computer technology companies have developed sophisticated risk-mitigation strategies to detect malicious code and deter its insertion into their global supply chains; the U.S. government needs to undertake a similar effort for critical civilian and military applications. – DEPSECDEF William J Lynn III, Sep-Oct 2010, Foreign Affairs

This is a problem that has been noted by DOD since the early 2000s. In 2005 the Defense Science Board completed an in depth study of the issue and concluded:

The microelectronics industry, supplier of hardware capability that underlies much of America’s modern military leadership technology, is well into a profound restructuring . . . One unintended result of this otherwise sound industry change is the relocation of critical microelectronics manufacturing capabilities from the United States to countries with lower cost capital and operating environments. Trustworthiness and supply assurance for components used in critical military and infrastructure applications are casualties of this migration.

These changes are directly contrary to the best interests of the Department of Defense for non-COTS ICs. The shift from United States to foreign IC manufacture endangers the security of classified information embedded in chip designs; additionally, it opens the possibility that “Trojan horses” and other unauthorized design inclusions may appear in unclassified integrated circuits used in military applications. More subtle shifts in process parameters or layout line spacing can drastically shorten the lives of components.
Summary

The United States Government is taking steps to elevate its response level to close the gap between the existing threat level and the current state of its operating assets. Achieving this goal in an accelerating threat environment will require a continued commitment of U.S. Agencies and increased investment in existing efforts and new programs.

In the shadow of substantial national software and signal-based initiatives there is another front to a potential cyber-war that is equally vulnerable but far less public, less discussed and certainly less funded. The data and traffic that is the focus of cyber security passes over a sea of computing and communication hardware devices whose performance is wholly dependent on myriad microelectronic semiconductor components. A new program to address the hardware aspect of cyber defense, a logical extension of the Trusted Foundry Program, would create the framework to provide this protection.

A new cyber hardware program would focus on the underlying microelectronics in Government information technology and communications networks. This activity would connect assets of the Trusted Foundry Program, the USCYBERCOM, the NSA, DHS, and other Government agencies vulnerable to cyber attacks such as the Departments of Treasury, Energy, and State.

Initial work would involve securing the hardware supply chain for the Government’s microelectronics in accordance with existing and expected Supply Chain Risk Management directives and policies. Future program initiatives will increase the nation’s cyber defenses by reducing the need for hardware component testing and eliminating complex software requirements to ensure network hardware’s viability.
Endnotes

1 Coleman, “Preparing for a Cyber Attack.” (12)

2 “Cyberwar: Sabotaging the System,” P.2. (13)


8 Lynn “Defending a new Domain.” (16)


10 Lynn, “Defending a new Domain.” (18)

Appendix A: Cyber Warfare Timeline: Selected Events

1969:

The Advanced Research Projects Agency launches ARPANET, an early network used by government research groups and universities, and the forerunner of the Internet. ¹

1972:

John Draper, aka Captain Crunch, discovers that the plastic whistle inside a box of breakfast cereal reproduces a 2600-hertz tone, a frequency that could be used to make free phone calls. He invents the “blue box,” a tone generator, which can unlock AT&T’s phone network, allowing free calls and manipulation of the network. ¹

1979:

Engineers at Xerox Palo Alto Research Center discover the computer “worm,” a short program that scours a network for idle processors. Originally designed to provide more efficient computer use, the worm is the ancestor of modern worms, destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted. ¹

1982:

Computer code stolen from a Canadian company by Soviet spies causes a Soviet gas pipeline to explode. The code is later proven to have been modified at the request of the U.S. Central Intelligence Agency, who had anticipated the theft, to include a logic bomb which changed the pump speeds to cause the explosion. ²

1983:

The FBI identifies and arrests the “414s,” a group of young hackers who break into several US government networks, in some cases using only an Apple II+ computer and modem. The incident appears as the cover story of Newsweek with the title “Beware: Hackers at Play,” possibly the first mass-media use of the term “hacker” in the context of computer security. As a result, the US House of Representatives holds hearings on computer security and passes several laws. ¹

University of Southern California doctoral candidate Fred Cohen coins the term “computer virus” to describe a computer program that can “affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself.” Antivirus makers later capitalize on Cohen’s research on virus defense techniques. ¹
1986:
One of the first PC viruses ever created, “The Brain,” is released by programmers in Pakistan.¹

1987:
The Christmas Tree EXEC worm causes major disruption to existing networks.¹

1988:
23-year-old programmer Robert Morris unleashes a worm that invades ARPANET computers. The small program disables 6,000 computers on the network by flooding their memory banks with copies of itself. Morris confesses to creating the worm out of boredom. He is fined $10,000 and sentenced to three years’ probation.¹

1988-1989:
Markus Hess, a young German computer expert, spends two years hacking into the ARPANET open network and MilNet, collecting data which he then sells to KGB agents in East Berlin. The intrusion is discovered by an American network user who notices a number of unusual connections with unlimited privileges giving access to most of the ARPANET/MilNet network.¹

1991:
Programmer Philip Zimmerman releases “Pretty Good Privacy” (PGP), a free, powerful data-encryption tool. The US government begins a three-year criminal investigation of Zimmerman, alleging he broke US encryption laws after his program spreads rapidly around the globe. The government later drops the charges.(1)
Symantec releases the Norton Anti Virus software.¹

An Air Force report indicates that a computer virus, “AF/91,” has been created and installed on a printer chip. The virus, designed to make Iraqi anti-aircraft guns malfunction made its way to Iraq via Amman, Jordan; however, sources indicate that the central command center was bombed and the virus destroyed. The virus, however, is found to be fake.²

The United States comes under attack from computers and computer networks situated in China and Russia. Government officials assign the code names “Titan Rain” and “Moonlight Maze” to these coordinated attacks.²
1994:

Inexperienced email users dutifully forward an email warning people not to open any message with the phrase “Good Times” in the subject line. The missive, which warns of a virus with the power to erase a recipient’s hard drive, demonstrates the self-replicating power of email virus hoaxes that continue to circulate in different forms today.¹

Russian crackers siphon $10 million from Citibank and transfer the money to bank accounts around the world. Vladimir Levin, the 30-year-old ringleader, uses his work laptop after hours to transfer the funds to accounts in Finland and Israel. Levin stands trial in the United States and is sentenced to three years in prison. Authorities recover all but $400,000 of the stolen money.¹

1995:

Microsoft releases Windows 95. Antivirus companies worry that the operating system will be resistant to viruses. Later in the year, however, evolved “macro” viruses appear that are able to corrupt the new Windows operating system.¹

1997:

The first high-profile attacks on Microsoft’s Windows NT operating system are launched.¹

1998:

Intruders infiltrate and take control of more than 500 military, government and private sector computer systems. The series of attacks, dubbed “Solar Sunrise” after the well known vulnerabilities in computers run on the Sun Solaris operating system, were thought to have originated from operatives in Iraq. Investigators later learn that two California teenagers were behind the attacks. The experience gives the US Defense Department its first taste of what hostile adversaries with greater skills and resources would be able to do to the nation’s command and control center, particularly if this form of cyber warfare were used in tandem with physical attacks.¹

1999:

The “Melissa” virus infects thousands of computers with alarming speed, causing an estimated $80 million in damages and prompting record sales of antivirus products. The virus starts a program that sends copies of itself to the first 50 names listed in the recipient’s Outlook email address book. It also infects Microsoft Word...
documents on the user’s hard drive, and mails them out through Outlook to the same 50 recipients.  

2000:

The “I Love You” virus infects millions of computers virtually overnight, using a method similar to the “Melissa” virus. The virus also sends passwords and usernames stored on infected computers back to the virus’s author. Authorities trace the virus to a young Filipino computer student who goes free because there are no laws against hacking and spreading computer viruses in the Philippines. This spurs the creation of the European Union’s Global Cybercrime Treaty.  

Yahoo, eBay, Amazon, Datek and dozens of other high-profile websites are knocked offline, some for several hours, following a series of so-called “distributed denial-of-service attacks” (DDoS). Investigators later discover that the DDoS attacks, in which a target system is disabled by a flood of traffic from hundreds of computers simultaneously, were orchestrated when the hackers co-opted powerful computers at the University of California-Santa Barbara.  

2001:

The “Anna Kournikova” virus, promising digital pictures of the young tennis star, mails itself to every person listed in the victim’s Microsoft Outlook address book. This relatively benign virus frightens computer security analysts who believe it was written using a software toolkit that allows even the most inexperienced programmer to create a computer virus.  

The “Code Red” worm infects tens of thousands of systems running Microsoft Windows NT and Windows 2000 server software, causing an estimated $2 billion in damages. The worm is programmed to use the power of all infected machines against the White House website at a predetermined date. In an ad hoc partnership with virus hunters and technology companies, the White House deciphers the virus’s code and blocks traffic as the worm begins its attack.  

Shortly after the 9/11 attacks, the “Nimda” virus infects hundreds of thousands of computers around the world. It is considered to be one of the most sophisticated viruses, with as many as five different methods of infecting systems and replicating itself.  

2002:

The “Klez” worm, a bug that sends copies of itself to all of the email addresses in the victim’s Microsoft Outlook address book, begins its march across the Internet. The worm overwrites files and creates hidden copies of the originals. It also attempts to
disable some common antivirus products and has a payload that fills files with all zeros. Variants of the “Klez” worm remain the most active on the Internet.\(^1\)

A denial-of-service attack hits all 13 of the “root” servers that provide the primary roadmap for almost all Internet communications. Internet users experience no slowdowns or outages because of safeguards built into the Internet’s architecture. But the attack—called the largest ever—raises questions about the security of the core Internet infrastructure.\(^1\)

2003:

The “Slammer” worm infects hundreds of thousands of computers in less than three hours. The worm wrecks havoc on businesses worldwide, knocking cash machines offline and delaying airline flights. It holds the ranking as the fastest-spreading computer worm ever.\(^1\)

2004:

The “MyDoom” worm becomes the fastest-spreading email worm as it causes headaches but very little damage, almost a year to the day after “Slammer” ran rampant in January 2003. “MyDoom” uses “social engineering,” or low-tech psychological tricks, to persuade people to open the email attachment that contains the virus. It claims to be a notification that an email message sent earlier has failed, and prompts the user to open the attachment to see what the message text originally said.\(^1\)

2006:

Israel alleges that, during its war against Hezbollah, cyber warfare was employed as part of the conflict; the Israel Defense Force (IDF) intelligence estimates that several countries in the Middle East used Russian hackers and scientists to operate on their behalf.\(^2\)

2007:

April - After riots in Estonia surrounding the relocation of a monument to the Red Army, the computerized infrastructure of that nation’s high-tech government comes under attack; experts call it a coordinated denial-of-service attack. A flood of bogus requests for information from computers around the world conspire to cripple the websites of Estonian banks, media outlets, and ministries for days.\(^1\)

The Russian Business Network (RBN) and their support units provide scripts and executables to make cyber weapons undetectable by antivirus software. Every time a copy of the cyber weapon is generated it looks different to the antivirus engines.
RBN’s cyber weapons are very popular and powerful. A RBN cyber weapon is used in June 2007 by a single person to attack and compromise over 10,000 websites in a single assault.  
McAfee, Inc. alleges that China is actively involved in “cyberwar.” China is accused of cyber-attacks on India, Germany and the United States, although China denies knowledge of these attacks.

September - Israel carries out an airstrike on Syria dubbed Operation Orchard. U.S. industry and military sources speculate that the Israelis may have used technology similar to America’s Suter airborne network attack system to allow their planes to pass undetected by radar into Syria. Suter is a computer program designed to interfere with the computers of integrated air defense systems.

The United States government suffers “an espionage Pearl Harbor” in which and “unknown foreign power…broke into all of the high tech agencies, all of the military agencies and downloaded terabytes of information.”

The website of the Kyrgyz Central Election Commission is defaced during its election. The message left on the website reads, “This site has been hacked by Dream of Estonian organization.” During the election campaigns and riots preceding the election, several denial-of-service attacks are launched against the Kyrgyz Internet Service Providers (ISPs).

2008:

January 18 – “Project Chanology” attacks Scientology website servers around the world. Private documents are stolen from Scientology computers and distributed over the Internet.

The Bush Administration establishes the Comprehensive National Cyberspace Initiative (CNCI) as a classified joint presidential directive. The initiative aims at coordinating policy, strategy, and guidelines to secure federal systems.

February – The U.S. Customs and Border Patrol announces the results of Operation Infrastructure (November and December 2007), during which agents seize 360,000 counterfeit integrated circuits and computer network components bearing more than 40 different trademarks.

March 7 – Chinese hackers claim to have gained access to the world’s most sensitive sites, including the Pentagon. They operate from a bare apartment on a Chinese island.

August – In conjunction with the military conflict between Russian and Georgian separatist forces, Georgia experiences a cyber assault that intermittently knocks its
national web presence offline. Multiple servers attack the Georgian government’s websites, modifying and blocking them. A group calling itself the “South Ossetia Hack Crew” claims responsibility for posting a series of images that compare Georgian President Mikheil Saakashvili with Adolf Hitler. Other official Georgian sites are affected, too.¹

The President of Georgia’s website is moved to the state of Georgia in the United States (hosted by Tulip Systems in Atlanta) as protection against threats both real and virtual. Georgian and pro-Georgia hackers counterattack and succeed in paralyzing several news outlets and agencies for several hours in the first 48 hours of the conflict.¹

Russian, South Ossetian, Georgian and Azerbaijani sites are attacked by hackers during the 2008 South Ossetia War.²

A hacking incident occurs on a U.S. Military facility in the Middle East. Pentagon officials indicate that a “malicious code” on a USB flash drive spread undetected on both classified and unclassified Pentagon systems, establishing a digital beachhead from which data could be transferred to servers under foreign control. “It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary. This...was the most significant breach of U.S. military computers ever and it served as an important wake-up call,” Deputy Secretary of Defense William Lynn writes in an article for Foreign Affairs.²

Reports indicate that the proliferation of cyber weapons has exploded and estimates suggest that over 70% of countries will have at least a basic arsenal of cyber weapons by the end of 2008.⁴

2009:

January – A cyber attack on three of the four internet service providers of Kyrgyzstan quickly overwhelms the services. Sources blame the Russian cyber militia and/or the Russian Business Network (RBN). RBN is thought to control the world’s largest botnet with between a 150 and 180 million nodes.⁵

March 28 - A cyber spy network, dubbed GhostNet, using servers based mainly in China, taps into classified documents from government and private organizations in 103 countries, including the computers of Tibetan exiles; China denies the claim.²

June – The United States DoD announces the formation of the U.S. Cyber Command. The United Kingdom announces its intention to form its own equivalent organization.⁶
July – A series of coordinated cyber attacks is launched against major government, news media, and financial websites in South Korea and the United States. While many believe the attack was directed by North Korea, one researcher traces the attacks to the United Kingdom. ²

December 2009:
A cyber attack, dubbed Operation Aurora, is launched against Google and over 20 other companies. Google says the attacks originated from China and that it will “review the feasibility” of its business operations in China following the incident. According to Google, at least 20 other companies in various sectors had been targeted by attacks. McAfee spokespersons claim that “this is the highest profile attack of its kind that we have seen in recent memory.” ²

Russia is believed to lead the world in moneymaking schemes on the Internet. A study by Sophos Labs estimates that a single online pharmacy can net 200 purchases a day or $16,000. A successful affiliate webmaster redirecting 10,000 hits per day to a scareware site can earn $180,000 a year. ⁶

2010:

January – South Korea launches a cyberwarfare command center in response to rumors of a similar move by North Korea. ⁶

March - The Obama administration publishes an unclassified summary of its Comprehensive National Cybersecurity Initiative (CNCI). ⁷

May – India imposes strict controls on telecom equipment made in China due to fears that hardware could be compromised with data-stealing components or software. ⁶

August – China orders its banks and major companies to limit use of foreign computer security technology, citing security concerns but thought to be shielding national companies from competition. The rules, dubbed Multi-Level Protection Scheme, direct that Chinese companies’ computer systems will be classified into five tiers of sensitivity; the top three must be supplied by companies owned by Chinese citizens. ⁸

September - Iran is attacked by the “Stuxnet” worm, thought to specifically target its Nantanz nuclear enrichment facility. The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyber warfare. ²

October - Iain Lobban, the director of Britain’s Government Communications Headquarters (GCHQ), says Britain faces a “real and credible” threat from cyber attacks by hostile states and criminals. Government systems are targeted 1,000 times
each month. Such attacks threaten Britain’s economic future. Lobban indicates that some countries were already using cyber assaults to put pressure on other nations.²

December – Germany announces it is planning to create a cyber defense center in 2011 to respond to increasing attacks on government institutions that are believed to originate mainly in China. Germany registered 900 attacks in 2009 and 1600 in the first 6 months of 2010.⁹

Endnotes:


Appendix B: National Cyber Initiatives

Summary of Comprehensive National Cyber Initiatives – Initiative Titles Only

• Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet.

• Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise.

• Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise.

• Initiative #4: Coordinate and redirect research and development (R&D) efforts.

• Initiative #5. Connect current cyber ops centers to enhance situational awareness.

• Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan.

• Initiative #7. Increase the security of our classified networks.

• Initiative #8. Expand cyber education.

• Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs.

• Initiative #10. Define and develop enduring deterrence strategies and programs.

• Initiative #11. Develop a multi-pronged approach for global supply chain risk management.

• Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains.

Source: