

March 15, 2010

## Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk

*In the span of three months during 2009, al Qaeda launched two separate, well-orchestrated attacks against the United States homeland that would likely have been devastating had they not been stopped. Nahjibullah Zazi, an Afghan raised in New York, recently admitted to a federal court that he conspired to detonate a bomb in the New York subway system around the eighth anniversary of September 11, 2001 — and was just days from putting his plot into motion. Zazi pleaded guilty to charges of conspiracy to use weapons of mass destruction, commit murder and provide material support to al Qaeda. This planned attack, had it occurred, would have been even deadlier than the July 7, 2005, attacks on the London Underground that killed 52 innocent people and injured 700, due to the larger, more lethal explosive devices that were to be used. The same could be said about Umar Abdulmutallab's al Qaeda-inspired plot to blow up Northwest Flight 253 on December 25, 2009.*

*The dangerous new phase in the fight against al Qaeda is, unfortunately, not limited to attacks on our transportation systems. Rather, the increasing globalization of our world, with its greater reliance on the Internet and heightened dependence on computerized automated systems, represents a massive and escalating vulnerability — particularly in light of al Qaeda's intention to harm the American economy. The Google attacks of December 2009 were a shocking breach of online security, while in late February 2010, a new "botnet" — a software agent that runs automatically, normally for malicious purposes — called the "Kneber botnet," was discovered to have infected more than 74,000 computer systems worldwide, compromising data from nearly 2,500 corporate and government networks in 196 countries. America now confronts a dangerous combination of known and unknown cyber vulnerabilities, rapidly expanding adversary capabilities, and — unfortunately — a lack of comprehensive threat awareness. This issue of The Lipman Report® will explore this new threat of cyberterrorism, analyze its methods and dangers and offer recommendations on how we can best protect ourselves.*

### How Vulnerable Are We?

In February 2010, America's top intelligence officials warned lawmakers that the threat of a crippling attack on telecommunications and computer networks was growing; an increasingly sophisticated group of enemies "severely threaten" the sometimes-fragile systems guarding the country's information infrastructure. These experts

warned that, "Malicious cyber activity is occurring on an unprecedented scale, with extraordinary sophistication." This threat illuminates the rising concern among American intelligence officials over the potentially catastrophic results of a coordinated attack on the nation's technology apparatus — appropriately called a "cyber-Pearl Harbor."

The threat of cyberterrorism to our technical infrastructure is real and immediate. Computers and servers in the United States are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency and sophistication each year. As our nation's critical infrastructure grows more reliant on information technologies, it has become more exposed to attackers, both foreign and domestic. These cyber-aggressors can threaten our nation's economy, public works, communication systems and computer networks.

Concerns over cyberterrorism arise from the fact that al Qaeda has expressed interest in devastating the United States economy — which is computer dependent — while Osama bin Laden has spoken of "bleeding America to the point of bankruptcy." Some experts feel that al Qaeda is not currently in a position to exploit this vulnerability; however, they allow that as with any developing technology, the costs and deterrents for developing an advanced cyber offensive are declining each year. Naysayers should also remember that the idea of using airliners as missiles to take down skyscrapers was also deemed unlikely and dismissed by authorities before the carnage actually occurred.

It is ironic that the Internet — a symbol to many of the open communication of our American culture — has evolved into a powerful tool for terrorists, who use online message boards and chat rooms to share information, coordinate attacks, spread propaganda, raise funds and recruit. The number of terrorist sites has increased exponentially over the last decade, from under 100 in the mid-to-late 90s to more than 4,800 over the last few years. Terrorist websites can serve as virtual training grounds, offering tutorials on building bombs, surface-to-air missile operation, surveillance, intelligence gathering and operational security. Terrorists have also developed sophisticated encryption tools and creative techniques that render the Internet an efficient and relatively secure means of correspondence.

If the pace of technology continues at this rate, greater technological change will occur in the next 20 years than

---

## Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk

occurred in the whole of the 20th century. The cyber domain is rapidly expanding the ability to create and share knowledge, but it is also enabling those who aim to steal, corrupt, harm or destroy public or private assets vital to national interests. The same technological advances that are benefitting us are also increasing the arsenal of our opponents. A wide spectrum of disparate groups is targeting American computer networks, including curious programmers, criminal outfits motivated by money, nation states, and terrorist and military organizations seeking to exfiltrate vast amounts of data from the United States public and private sectors.

In the recent “Kneber Botnet,” hackers gained access to a wide array of data, from credit card transactions to intellectual property. In more than 100 cases, they also infiltrated corporate servers that store large quantities of business data, such as company files, databases and e-mail. The computer systems of more than a few Fortune 500 firms were compromised. The damage is still being assessed, and affected companies are still being notified. According to experts, this grand-scale cyber operation began in Germany in 2008, with a familiar type of “phishing” attack designed to get corporate insiders to click on phony links that would ultimately install malware on the PCs, granting the hackers remote control access to their computers, and ultimately to their networks.

The national security of the United States — its economic prosperity and the daily functioning of its government — are dependent on a dynamic public and private information infrastructure of increasingly broad and complex telecommunications and computer networks. Even more worrisome, network technology favors the malicious actors over the protective systems we have in place, allowing the attackers to control open access to the Internet and establishing, in effect, an information-age Berlin Wall.

### **Cyberterrorism**

One of the most alarming incidents in 2009 was the July 4 assault on United States government sites — including the White House, the New York Stock Exchange and NASDAQ — followed a few days later by similar attacks on websites in South Korea. According to a research paper by a leading antivirus maker, both attacks were made by the same botnet of 50,000 computers, which spammed targets with such a large number of e-mails that their IT systems were simply overwhelmed. In his “Annual Threat Assessment of the United States Intelligence Community,”

Director of National Intelligence Dennis Blair postulated that this attack might have been a cyber “dry-run” to test the impact of flooding South Korean networks and transcontinental communications on the part of North Korea — as previously occurred in Estonia in 2007 and the Republic of Georgia in 2008 — giving them significant advantage in the event of a surprise attack. Experts need to remain aware of this type of “trial” threat from state-sponsored actors — who are just seeking out vulnerable points and analyzing responses in preparation for the next, larger-scale operation.

It is clear that terrorist groups and their sympathizers intend to use cyber means to target the United States and its citizens. The initial, limited success of these groups may serve to embolden future hackers to attack critical infrastructure — such as power generators or air-traffic control systems — with devastating consequences for the United States economy and national security. As their skills naturally sharpen, cyberterrorists will begin to attack high-value targets, through the interception of confidential communications and modification of critical data, resulting in both physical harm and denial of resources in times of crisis. Since terrorists groups such as al Qaeda have demonstrated they are capable of thinking outside the periphery of our mental boxes, the weapon of choice by governments, corporations and individuals must be a well-prepared security plan, one that includes risk assessments, physical surveys and business continuity elements, to both prevent and minimize the consequences of cyberattacks.

### **Dangerous Scenarios**

Somewhere in the United Arab Emirates, Iran, Indonesia or Malaysia, it is likely that there are technical computer specialists working towards mastery of the global information infrastructure. Malaysia, for example, is emerging as a cyber-sanctuary for pro-al Qaeda hackers and virus writers. Their goals are simple: to bring down high-value targets that represent Western power and so-called Western aggression over Muslims. Possible targets might be regional power grids or the stock exchange, anything that relies on a computer network infrastructure for its continued operations. Then, when a physical attack — such as a bomb — occurs immediately after, the fatalities and damages that ensue in the face of these heightened system vulnerabilities would be that much worse. Such is the raw potential to attack individuals, organizations, infrastructures and key economic sectors in a modern digital world — with a few keystrokes aiding physical aggression.

---

The emergence of a cyberterrorist facilitating physical acts of violence brings a host of implications about the future of electronic security. The vulnerabilities that continue to exist throughout the telecommunications system — such as telephone, mobile access, cable, satellite and the Internet — are tempting targets. Sectors such as public and private facilities, banking and finance, transportation, manufacturing, medical, education and government are all dependent on the global information infrastructure for daily operations and may easily fall victim to cyberterrorists.

#### **How it Works**

Cyberterrorism is a controversial term, but can be defined generally as the premeditated use of disruptive activities — or threat thereof — against computers or networks, with the intention to cause harm, intimidate, or further social, ideological, religious or political objectives. To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause sufficient harm to generate fear. The attack need not be merely the theft of information, but can — through the manipulation of computer systems — lead to death or bodily injury, explosions, plane crashes, water contamination or severe economic loss. Globally, widespread cyber-facilitated bank and credit card fraud has serious implications for economic and financial systems, along with the national security, intelligence, and law enforcement communities charged with protecting them.

While providing greater efficiency and services to users, two global trends within the information technology environment potentially increase the vulnerabilities and consequences of security failures. The first is network convergence — the merging of distinct voice and data technologies to a point where all communications: voice, facsimile, video, computers, control of critical infrastructure and the Internet, are transported over a common network structure. This convergence amplifies both the opportunity for and consequences of disruptive cyberattacks. The second is channel consolidation, the concentration of data captured on individual users by service providers through e-mails or instant messaging, Internet search engines and Web social networking, which all increase the potential exploitation of personal data by malicious entities. The heightened interconnection of information systems and data inherent in these trends pose great threats to the confidentiality, integrity and availability of critical infrastructures, and to secret credentialing and identification technologies.

#### **Cyber Shock Wave**

Recently, a mock exercise developed by former CIA Director, General Michael Hayden, and the Bipartisan Policy Center's National Security Preparedness Group — titled Cyber Shock Wave — was held in Washington, D.C. The fictitious Cyber Shock Wave scenario was a simulation that took the form of an attack in a single day, via a malware program on 20 million smartphones. The simulation predicted a disruption of mobile service that would spread to take down the Eastern seaboard power grid and an energy-trading platform. In this imaginary attack, spyware used to funnel millions of dollars to banks overseas would be loaded onto smartphones. The malicious application would then add the infected phones to a telecommunications botnet, which would then in turn flood data networks of major carriers, slowing them to a crawl before disabling them completely. To make matters worse, the malware on the smartphones would begin to replicate, infecting all connected computers. In the end, all communications systems would be crippled. If this weren't enough, weather patterns resulting in a heat wave and hurricane were built into the simulation, to further add confusion and to stress the electrical system.

A malicious application causing harm to telecom and computer systems is one scenario that is highly likely, as more applications emerge in the market and more people switch to smartphones. Unfortunately, however, the former top United States officials role-playing in this mock scenario were virtually clueless, and after extensive debate had no real answers to prevent this impending disaster. This simulated large-scale attack revealed that the United States is ill-prepared to deal with such a threat and urgently calls for a solid level of cooperation inside the government, as well as between the government and the private sector.

#### **Wake-Up Calls**

This recent surge in cyberattacks was a “wake-up call” to those who dismiss the threat of computer warfare and cyberterrorism. Sensitive information is stolen daily from both government and private-sector networks, undermining confidence both in our online communication systems and in the very information these systems were intended to convey.

In a statement reported in an internationally published Pakistani newspaper following the September 11 attacks, Osama bin Laden said that thousands of Muslim scientists were using their knowledge in

## Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk

chemistry, biology, computers and electronics to wage war against the infidels. The Osama bin Laden Crew (OBL Crew), a group of self-proclaimed cyber jihadists, was reportedly founded in 2000 by Abdullah Qureshi, an al Qaeda member last reported to be living in Germany. The group's activities have consisted of the creation of dozens of websites and forums that provided information on weapons and explosives and facilitated large-scale recruitment efforts and propaganda.

Other cyberterrorism "wake-up calls" include:

- The terror alert in August 2004 detailing al Qaeda's plans to attack financial institutions in New York and New Jersey. This came after the arrest in Pakistan of Muhammad Naeem Noor Khan, a computer engineer.
- Abu Anas al-Liby, one of al Qaeda's ranking computer experts, trained agents in computer surveillance techniques, according to testimony in 2001 in the Nairobi embassy bombing trial.
- Encrypted, detailed plans for destroying airliners were found on Ramzi Yousef's laptop computer. He helped to plan the 1993 World Trade Center bombing.
- Osama bin Laden's aides utilized encrypted e-mail to transmit the 9/11 attack instructions to Mohammed Atta.
- Supervisory control and data acquisition (SCADA) system websites have been accessed by al Qaeda members in order to gather intelligence on these potential targets. SCADA systems are used to monitor and control utility equipment, such as power and water distribution systems.
- Al Qaeda-owned computers were found to have structural and engineering data associated with dams.
- Khalid Ibrahim, a member of the Pakistani terrorist group Harkat Ul Ansar, is known to use social engineering methods to gain information on hacking into United States military networks.
- Al Qaeda prisoners, during interrogations, have stated their intentions to use computer network tools to further their goals.
- Many of the actors in recent foiled plots were discovered to have been radicalized online, on terrorist websites and in al Qaeda chat rooms.

Jihadist terror is becoming a wide-open field, as witnessed by the almost daily carnage throughout the world caused by suicide bombers in the cause of Islamic extremists. After September 11, many experts were skeptical about the threat of jihadist cyberattacks aimed at disrupting key sectors of the economy that are driven by computers, such as banking

or telecommunications. Their belief was that this type of attack would not interest jihadists because of the lack of direct bloodshed — bloodshed that seemed a prerequisite of the new terror. But that judgement was — unfortunately — premature. Current online forums appear devoted to "e-jihad." There has been some hacking of websites by Islamic extremists, and those who frequent Islamic message boards express a desire to improve jihadist cyber skills.

Computers and servers in the United States are the most aggressively targeted information systems in the world, with attacks increasing in severity, frequency and sophistication each year. As our nation's critical infrastructure grows more reliant on information technologies, it also becomes more exposed to attackers, both foreign and domestic. These attacks can threaten our nation's economy, public works, communication systems, and computer networks — and a computer and a connection to the Internet are all that is really needed to wreak havoc. Compounding the problem is that both the public and private sectors remain relatively ignorant of their rising dependence on computer systems.

*Cyberterrorism is a real, often stealth danger that needs to be examined, not only by information technology officials, but by anyone who uses a computer network of any kind. To stay ahead of al Qaeda and other malicious actors, the United States needs to make targeted investments to bolster the security of its critical infrastructure — starting with government and military systems, but extending into the private sector, particularly into the electric grid and financial community. What is required today is a sense that individually, we need to secure ourselves first, then rely on others for security. We should not assume that we live in a protected American cyber enclave; cyberterrorism must be treated as a threat equal to that of weapons of mass destruction, and given the same priority attention. We need to respond with a full understanding of the cyber threat, a proactive defense posture and strategic efficient preparedness plans that take into account the ever-changing nature of this new menace. **The time for urgency is now.***



The Lipman Report Editors