

September 15, 2009

---

## The Rising Tide of Cyberwarfare: Cyberterrorism and Cybercrime in a Climate of Heightened Global Risk and Economic Instability

*Since 9/11, known and potential attacks on the Internet by hackers, criminals, and foreign and domestic terrorists have produced an ominous new term: cyberwarfare. The development and identification of this new threat has taken place over the past four decades, since 1969 when the global Internet's first conceptually simple step was taken — the experimental, reluctant linking of several computers in a few scientific centers across the United States so that they could communicate with one another. These humble beginnings spawned the hundreds of thousands of Internet hosts and billions of Web pages we navigate today, tracked by an array of search engines — a virtual spider web of communication and data information that seems to grow exponentially with each passing second. As with many developments that take hold quickly, however, the issue of security initially fell by the wayside. The original builders of the Internet concentrated on protecting the network from physical attack, not electronic attack, while focusing on utility and rapid innovation.*

*Compounding this very real problem is that America has since become a nation almost entirely dependent on cyberspace. The vulnerable Internet servers have become the arteries and veins of the national critical infrastructure. On these relatively unsecured connections rest the safe operations of our nearly 7,500-mile border with Canada and Mexico, crossed each year by more than 500 million people, 130 million motor vehicles and 2.5 million railway cars. Internet connections also monitor the patrolling of almost 9,500 miles of shoreline and navigable waters, along with 361 ports that annually see 8,000 foreign-flag vessels, nine million containers of cargo and nearly 200 million cruise and ferry passengers. The list of Internet-dependent United States security operations seems endless; there are 442 primary airports and 124 commercial service airports that see 3,000 flights and 1.8 million passengers every day with schedules relying on proper online communication. There are approximately 4 million miles of highways and streets and 220,000 miles of rail track crisscrossing the nation, while 590,000 bridges, 54,000 community water systems and 75,000 dams dot America's biggest cities and smallest towns. Moreover, in an overlapping and sometimes confusing system of federal, state and local governance, the United States operates more than 87,000 different police jurisdictions, 26,000 fire departments and some 6,000 hospitals — all of which are connected*

*to and dependent on the Internet. Not the least of our concerns is the degree to which our financial systems, structures and operations are Internet-dependent.*

*It is against this convoluted, easily targeted backdrop of Internet data transmission and operational communications that the war on terrorism began in September 2001 — setting the stage for a cyber battlefield. Moreover, recent and current economic problems make the Internet a tempting vehicle for cybercrime — online piracy of valuable data and resources belonging to individuals and corporations. This issue of The Lipman Report<sup>®</sup> will explore and analyze the evolving threat of both cyberterrorism and cybercrime and make recommendations for how we can best protect ourselves against these vulnerabilities.*

### **Cyberterrorism**

Cyberterrorism is defined as the “premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention of causing harm to further social, ideological, religious, political or similar objectives.” It is the leveraging of a target's computers and information, via the Internet, to cause physical, real-world harm, perceptual disturbances or severe disruption of infrastructure. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunication systems to exchange information or make threats electronically. Examples include: hacking into computer systems; introducing viruses and worms to vulnerable networks; Web site defacing; denial of service attacks — a classic hack that attempts to overwhelm targeted sites with massive amounts of data and thus freezes out access by anyone else, thereby crippling the entire network — or terrorist attacks made via electronic communication. The intent of a cyberterrorism attack may be to cause economic disruption through interruption of financial networks, generate logistical disruptions to create chaos or support a concurrent physical terrorist attack as a means of causing further confusion and delays in response.

Flexible and simple for terrorists, spies and criminals, the Internet is a ready vehicle with which to spread violence and fear, and to plan and carry out attacks. The Web allows for easy access to a wealth of sources around the world with little or no regulations, censorship or other forms of government control. It also

---

## The Rising Tide of Cyberwarfare: Cyberterrorism and Cybercrime in a Climate of Heightened Global Risk and Economic Instability

caters to large audiences and allows for anonymity of communication and a rapid flow of information. Moreover, the development and maintenance of a Web presence is easy and inexpensive — one does not need sizable resources to create a multimedia environment with the ability to combine text, graphics, audio and video. The Internet is also a natural tool with which to shape coverage in the traditional mass media, which is relying increasingly on “the information superhighway” as a primary source for their stories.

The immediate aftermath of 9/11 generated several fears about the role that the Internet and networked computers might play in a terrorist attack. The reasoning is that those who seek to threaten American national security could do so with greater ease and effectiveness if they obtained weapons system information or substantial financial information from banks online. In response to this very realistic threat, an entire industry has emerged to grapple with the threat of cyberterrorism. Non-government companies have hastily deployed security consultants and software designed to protect public and private targets. The federal government requested \$4.5 billion for infrastructure security following 9/11, and the FBI now boasts more than 1,000 “cyber investigators.”

The term “cyberterrorism” creates a subliminal linkage to groups such as al Qaeda and other global jihadists. Al Qaeda and other terrorist groups are very much aware that they cannot confront the United States military on traditional battlefields; however, disrupting our information infrastructure through online attacks is far less risky. A desktop allegedly used by Ayman al-Zawahiri — Osama bin Ladin’s top deputy — that fell into the hands of coalition forces in November 2001 contained nearly 1,000 text documents, photographs and video files, along with hundreds of Web pages, many of which were part of the group’s intensifying efforts to conduct a global Internet-based publicity and recruitment effort. Muhammad Naeem Noor Khan, the alleged al Qaeda computer expert arrested in Pakistan in August 2004, told United States government investigators that al Qaeda members use e-mail and Web sites in Turkey, Nigeria and the Pakistan tribal regions to communicate. Muhammad Khan’s hard drives were filled with Web pages and images that were gathered to conduct surveillance, select targets and plan attacks. These revelations illuminated the fact that our enemies

are taking advantage of the free, open, information-rich American society to mine the Web for data — it is just simple logic that terrorists can “Google” too.

Terrorist use of the Internet and other telecommunication devices is sharply on the rise around the globe. Since 9/11, there has been a tenfold increase in the number of terrorist sites online. Prior to the September 11 attacks, there were 70 to 80 terrorist sites, whereas now there are around seven to eight thousand — correlating directly with the growth of the Internet since 2001. These Web sites are spreading militant propaganda and proselytizing violence to every corner of the world. The FBI Director recently revealed that terrorists are relying more heavily on the Internet than ever before to communicate, conduct operational planning, recruit and train, and to obtain logistical and financial support. Moreover, reports indicate that terrorists and extremists in the Middle East and South Asia may be collaborating more frequently with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs.

Historical examples of mass cyber attacks on a national basis include the 2007 cyber attack on Estonia in the wake of the removal of a Russian World War II memorial from downtown Tallinn, Estonia, and the more recent event in 2008 when a massive “denial of service” cyber attack paralyzed the Republic of Georgia during its controversy with Southern Ossetia. These are extreme examples, but they attest to the power of the Internet when used for nefarious purposes. However, the worst-case scenario envisions a Web Pearl Harbor that catches us by surprise and crashes our financial markets, or kills thousands of people trapped in computer-controlled transportation systems or high-rise elevators run amok, or generates a blackout in a city facing a blizzard or heat wave, or targets preterm babies in microprocessor-controlled incubators by crashing their life support.

One example of our current vulnerability is the fact that the location of 180,000 miles of gas pipelines crisscrossing the United States can be easily accessed on the Internet. One would think that this would be closely guarded information, but private industry and local governments have publicized the locations of natural gas pipelines to make them safer because misdirected backhoes and wayward boat anchors have caused scores of lethal explosions in the past. Since 9/11, security concerns have dictated a rethinking of

this openness — there are over a billion Internet users, and clearly not all of them are friends.

Terrorism is violence used to create shock and achieve political objectives. A cyber attack, which may not even be noticed by its victims or may be attributed to routine delays or outages, may not seem at first glance to be a terrorist's preferred weapon. Many argue that a simple homemade bomb is always going to be more effective as a terrorist weapon than an electronic attack with an impact that may be gradual, cumulative, and of limited duration, but others claim it's only a matter of time before a terrorist group manages to bring down a critical structure such as an air-traffic control system with a cyber attack, potentially killing millions. Furthermore, the threat of a cyber attack as a vehicle to create a diversion or add confusion to the site of a concurrent physical attack — creating chaos and impeding response — is a very real one.

#### **The recent rise in cybercrime**

The threat and reality of online criminal activity is currently even greater than that of cyberterrorism; whether people realize it or not, the world is already subject to being held hostage by cybercriminals. Since the dawn of the Internet, cyberspace has witnessed unauthorized intrusions and Web hacks from a myriad of actors: teenagers, industrial espionage experts, hacker groups and nation states. Newcomers have infiltrated very sensitive systems with relative ease, utilizing a host of weapons that have a language of their own: social engineering, dumpster diving, trashing, viruses, worms, Trojan horses and denial of service attacks. Every day, criminals are invading countless homes and offices across the nation — not by breaking down windows and doors, but by worming their way into laptops, personal computers and wireless devices via hacks and bits of malicious code. The new Conficker program, which has already invaded millions of computer systems in 200 countries, quietly brings these computers under the control of a remote system, stealing personal data and passwords from the infected computers.

Billions of dollars are lost every year from such attacks. Some of the direct cost implications of cyber attacks are: the cost of repairing systems after an attack, loss of sales during an interruption, increased insurance and mounting forensic investigation and litigation costs. The indirect cost implications are also significant: loss of confidence and credibility in our financial systems, tarnished relationships and public image, loss of future

customer revenues, strained business partner relationships and reduced trust in the government.

Fifteen years ago, the FBI mounted its first major cybercrime investigation. An organized crime group in the former Soviet Union was able to hack into the Internet system of a major Western bank, transferring large sums of money internationally and allowing members of this group to access the money. Fortunately, suspicious bank officials notified the FBI regarding the unlikely characters that were poised to collect hundreds of thousands of dollars. The human factor thwarted this attempt; however, the new, more sophisticated generation of cybercriminals that has since surfaced poses a far more significant threat.

Online scammers have been ramping up their efforts with fraudulent schemes designed to take advantage of public confusion over banking consolidations and prey on mass concern and desperation over stock market declines, mounting layoffs and unexpected foreclosures. There are, in fact, direct correlations between targeted cyber attacks on consumers and the stock market decline over the past year. While the United States stock market saw catastrophic declines in mid-to-late 2008, the volume of malware threats — “malicious” software designed to infiltrate or damage a computer system without the owner's active consent — more than doubled. According to a report from an international network of support centers designed to protect users against viruses, cybercriminals increase their activity to siphon funds away from unsuspecting online victims during times of economic instability. The study also reported a surge in the number of fake antivirus software scams tricking unsuspecting consumers into making online transactions, generating an estimated \$14 million in profit each month for cybercriminals.

Consumers are being victimized in a number of ways. In one type of online scam, called “phishing,” criminals masquerade online as trustworthy entities in order to gain confidential information such as Social Security numbers, dates of birth or credit card numbers. One current phishing scheme involves e-mails asking people to provide their bank account information so as to avoid having their bank account closed in a merger. Soon after providing their bank account details, these victims find that their account balance is wiped out. In another type of scam, cybercriminals advertise purported work-from-home “jobs” on the Web, “jobs” which are actually heists

## The Rising Tide of Cyberwarfare: Cyberterrorism and Cybercrime in a Climate of Heightened Global Risk and Economic Instability

in disguise. In one recent such scam, an advertiser masqueraded as a foreign-based corporation recruiting individuals to act as fiduciary agents by depositing funds in their personal accounts, then wiring the proceeds — less a “commission” — to an offshore account. The victim would deposit the phony check in his or her personal account, and since the counterfeit checks looked legitimate, the bank would credit the account with the funds. Only after the checks made it to the Federal Reserve Bank, which took upwards of two weeks, were they discovered to be counterfeit. By this time, the victims had already wired money from their accounts via Western Union to “company representatives” offshore, but since the “cashier’s checks” were fake, the victims had to absorb the losses to the bank. These transactions amount to nothing more than a money laundering move, known as a “cyber mule operation.”

Increased economic woes have also generated a rise in data theft. Displaced employees are using their corporate data access to steal, exploit and damage information networks, potentially costing businesses as much as one trillion dollars globally. While insiders have always posed a threat to information security, reports indicate that current economic pressures are putting vital information at greater risk than ever before. In the wake of a year of massive layoffs, employees shown the door can be tempted to leave the premises with valuable intellectual property to bolster their chances of finding a job with a competitor, to use with a start-up company of their own or perhaps even to sell. This problem is exacerbated by the fact that businesses cutting staff and budgets over the past year to try to stay afloat in the challenging economy often cause management chaos within IT groups. Employees may be unsure of how and to whom to report security concerns, and existing controls may not be monitored as roles are switched and jobs lost. Workers may also be reluctant to report security issues for fear of jeopardizing a co-worker’s job or drawing unwanted attention to themselves. Not surprisingly, ignoring security problems can be costly; the average security breach results in a loss of millions of dollars in intellectual property and costs hundreds of thousands of dollars to clean up.

Computer crime issues have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography and online child grooming — the act of befriending a child online with the intention of eventual sexual abuse. Computer and

information security, data protection and privacy are all growing problems. The social, economic and even physical implications of a major cyberterrorism attack against our infrastructure are unthinkable. Actively protecting our computers, information and communications networks secures the economy and the country, keeping businesses, organizations, finances and people safer. A global strategy and policy for combating this criminality and terrorism is needed now. This requires a shift in mindset; not just the problem of an IT staff, information security is the responsibility of all employees of an organization — from the bottom to the top.

Security training and awareness programs should be mandatory at all levels — from executives to clerical staff — while strong senior management support for such programs is vital to ensure they are adhered to and taken seriously. Some valuable steps include: educating employees on reporting suspicious computer activity, deactivating computer access for terminated employees and implementing strict password and e-mail account management policies. Educating employees on what can go wrong and instituting an efficient protocol for the timely reporting of suspected problems are also essential steps.

*As the Internet continues to expand and computer systems are delegated even greater importance and responsibility in our society — while becoming ever more complex and interdependent — sabotage or terrorism via cyberspace has evolved into a weighty threat. Our open, capitalist way of life brings prosperity and fulfillment to many, but also results in levels of national vulnerability not found in other, more authoritarian societies. Consequently, these vulnerabilities must be managed carefully to ensure that the inevitable risks are tolerable, and that our enemies’ work is not made easier because of insufficient education, poor risk management or a fatal lack of attention to the larger picture. In our climate of mounting risk from both international and financial adversaries, now is certainly not the time to sacrifice security for utility, or long-term safety for immediate reward. **The time for urgency is now®.***



The Lipman Report Editors