IS THERE A CYBERSECURITY THREAT TO NATIONAL SECURITY: AN INTERPRETIVE ANALYSIS

Sean P. Gorman*

School of Public Policy,
George Mason University
Fairfax, Virginia 22003, U.S.A.
*Corresponding author
e-mail: sgorman1@gmu.edu

Cybersecurity has received an increasing amount of attention as an area vital to national security. While the vulnerability of cyber assets is well documented there is less research examining what the possible threats are and what level of prevention they warrant. An assessment of threats to cybersecurity and analysis of when cyber related assets have failed or been compromised is endeavored by this paper utilizing interpretive analysis. The conclusion will be put in the context of institutions with jurisdiction over the issue.

Introduction

Since the events of 9/11 there has been increased attention to cybersecurity as an important facet of national security and critical infrastructure vital to the functioning of the United States economy. The Whitehouse's National Strategy to Secure Cyberspace states that:

> By 2002, our economy and national security are fully dependent upon information technology and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy – (CIPB 2003, p.3)

Cybersecurity is also highlighted as an area critical to national security by the National Research Council, Critical Infrastructure Protection Board and the National Security Telecommunications Advisory Committee (CIPB 2003, NRC 2002b, NSTAC 2002). This point, though, has not been without contention, especially in regards to the threat posed by cyberterrorism. Green (2002) maintains there is a "myth" of cyberterrorism in the current administration:

> "There is no such thing as cyberterrorism--no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer. Nor is there compelling evidence that Al Qaeda or any other terrorist organization has resorted to computers for any sort of serious destructive activity (p.1).

To analyze whether there is a threat to national security posed by cybersecurity both sides of the issue will be analyzed and a range of potential threats will be discussed including terrorism along with analysis of when critical infrastructure has failed and the effect. The analysis is interpretive based on a wide variety of public documents and media outlets since there are little written in the academic literature on the specific topic. Firth the case against cyberscurity as a national security threat, specifically in regards to terrorism is presented.

Green's (2002) myth of cyberterrorism opened a policy debate on the issue of cybersecurity in the context of national security, specifically analyzing the possible threat of terrorists implementing a cyber attack on the United States. Berinato (2002) extended Green's argument stating that terrorist organizations like Al Qaeda will follow the path of least resistance and physical attacks and bombs offer a cheaper and easier alternative than the sophistication of a cyber attack. Even the use of cyber attacks to control physical infrastructure electronic systems has only been considered as a worst-case scenario causing minor inconvenience. Largely these reports have been from investigative reporters relying on interviews with "experts" in the field like Georgetown University Professor Dorothy Denning, "Not only does [cyberterrorism] not rank alongside chemical, biological, or nuclear weapons, but it is not anywhere near as serious as other potential threats like car bombs or suicide bombers (Green 2002, page 2)."

A more analytic approach was taken by the Unites States Naval War College in conjunction with Gartner Research to simulate a "digital Pearl Harbor" attack against the nations critical infrastructures. The study found that:

> A group of hackers couldn't single-handedly bring down the United States' national data infrastructure, but a terrorist team would be able to do significant localized damage to U.S. systems (Kane 2002 p.1).

The results had a further caveat that such an attack would require $200 million in funding, country-level intelligence and five years of preparation time. Whether there is an enemy that could under take such an offensive is an open question. Is there a realistic national security threat posed by critical infrastructure and cybersecurity, or is it a myth that has been over sold for various reasons. To date most available evidence of cyber threats in the public domain is anecdotal. It is useful, though, to examine the anecdotal evidence of critical infrastructure threats. To provide some structure to the wide range of attack examples considered they are divided into physical failures, unintentional and intentional, and malicious cyber attacks and developing cyber warfare capabilities.

Attack of the Backhoes and Massive Physical Telecom Failures

While cyber attacks tend to get the majority of media coverage, it is also important to note damage of critical infrastructure from physical failures. Physical failures in the telecommunications grid are probably the most frequent on a day-to-day basis, resulting largely from accidental fiber cuts from backhoes and shovels. The prevalence of accidental fiber cuts can be seen in the number of local "call before you dig" and "Miss Utility" programs. While most of these cuts result in minor inconveniences like the loss of localized service, several cuts have resulted in major outages. Fiber cuts have often plagued airport air traffic control. In 1990 a fiber cut shut down Chicago's O'Hare airport and the following year a cable cut in New Jersey shut down all three New York airports and caused air traffic control problems from DC to Boston (Neuman 1991). Fiber cuts often also reveal the interdependency of several critical infrastructures, the same fiber cut that shut down New York City's airports also shut down the NY Mercantile Exchange and hampered long-distance calling for nine hours (Neuman 1991). Further, fiber cuts can often be time consuming to repair, in 2000 a San Jose cut left customers out of service for over a week, "The repair work is mind-numbingly tedious, with each wire having to be spliced by hand and then tested (Neuman 2000)." More recently a train derailment and chemical spill in the Baltimore Howard St. tunnel slowed down Internet traffic coast-to-coast. While the robust SONET ring technology employed by several providers who lost circuits did reroute traffic in short order, the flood of rerouted traffic along poorly capacitated alternate routes slowed down traffic as far away as Seattle and Los Angeles (Lindstrom 2001).

The Impact of Telecommunications Failure during 9/11

The single largest physical loss of telecommunications infrastructure was the fall of the world trade center towers on 9/11. FCC records report that Verizon alone had to

replace 1.5 million voice circuits, 4.4 million data circuits, and 19 SONET rings, also 112,000 private branch exchange trunks, and 11,000 fiber lines dedicated to Internet service providers were destroyed (FCC 2001, GAO 2002). Further, Verizon lost its primary central office, 140 West St., resulting in the loss of telecommunication service to 34,000 businesses, including the New York financial district (GAO 2002). The loss of the Bank Of New York's primary data center caused nearly $80 billion in securities trades to fail (Newman 2002). Following the destruction of 9/11 the Federal government's calls for firms to locate backup facilities 120 miles from Manhattan were rejected by the financial community and most vulnerabilities are considered to still be unfixed (GAO 2002, Newman 2002). The vulnerabilities of fiber diversity has been well noted by the government as early as 1995:

> The use of optical fiber increases the effects of strategic sabotage attacks because optical fiber technology is diminishing the number of geographic transmission routes, increasing the concentration of traffic within those routes, reducing the use of other transmission technologies and restricting spatial diversity (NIST 1995, page 23).

While their have only been a few documented cases of fiber sabotage their effect has been dramatic. Over the past two years the Seattle area has been plagued by a fiber saboteur who has taken out 911 services four times with strategic fiber cuts (Halsne 2003). The most recent cut on September 3, 2003 disabled 911 services for nearly 9 hours and the perpetrator remains at large (Halsne 2003). There is often a somewhat mistaken belief that fiber networks are fully redundant rings that would prevent these types of cuts from disrupting critical resources. In an August 5th, 2003 court case involving the Maine Public Utility Commission an expert witness from Verizon stated that only 10% of the fiber rings in Maine are fully redundant, and 90% are at least partially collapsed and vulnerable to single cut failures (Maine PUC, 2003). Further, the standard operating procedure for restoring a failed line is to locate the lead engineer for the region, consult paper maps, manually identify an alternate route, and send technicians to wire jumper around the outage (Maine PUC, 2003). While the difficulties imposed by dependence on telecommunications fiber and anecdotes of fiber failures are well documented there has been little organized effort to quantify the impact of the vulnerability at a national level.

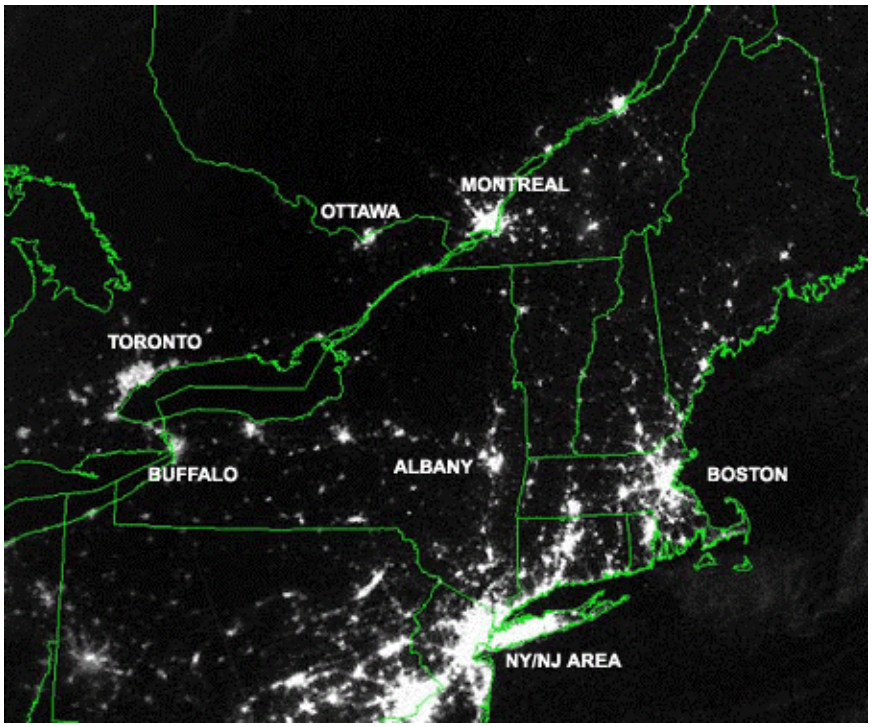
Lights Out

Cyber assets do not operate in a vacuum, but are interdependent with other critical infrastructure like electric power; as such it is useful to examine these interdependencies and the result of failures. While physical telecommunication failures may be the most common, by far the most obvious to the public are electrical power grid failures. The huge Northeast blackout on August 14th 2003 is one of the largest and most recent it is far from singular:

> On 10 August 1996, faults in Oregon at the Keeler-Allston 500 kV line and the Ross-Lexington 230 kV line resulted in excess load, which led to the tripping of

> generators at McNary Dam, causing 500 MW oscillations, which led to separation of the North-South Pacific intertie near the California-Oregon border. This led to islanding and blackouts in 11 U.S. states and 2 Canadian provinces and was estimated to cost $1.5 billion to $2 billion and included all aspects of interconnected infrastructures (Amin 2001, page 22).

The huge outage in 1996 was caused inadvertently by sagging power lines that came in contact with untrimmed trees causing the lines above to short. Other large-scale power outages include the northeast blackouts of 1977 and 1965. Since the outage of 2003 is most recent it warrants a closer look into it causes and effects. The conditions during the 1996 and 2003 blackout were quite similar. Both occurred during August when power consumption is at a peak along with the summer heat. As with the 1996 outage over capacitated lines resulted in a cascading failure that spread throughout the region. In the case of the 2003 outage the series of events began with FirstEnergy's Eastlake coal generation plant tripped off, sending a puff of ash spewing into the local neighborhood. An hour after the coal plant failure the Chamberlin to Harding power line tripped, which caused the power from it to be rerouted to the Hanna to Juniper line (PSERC 2003). When lines like the Chamberlin line fail it can be problematic because energy in an electric power grid cannot be stored or slowed down, but must be immediately routed to alternate paths in the network. Under conditions of high utilization of power lines there is not excess capacity to absorb the rerouted power from a failed line, causing the alternate path to fail. This sequence can be the start of a domino effect cascading power throughout the network over capacitating lines causing an entire grid failure. This is the scenario that caused the 2003 blackout. The Hanna to Juniper line could not absorb the rerouted power from the failed Chamberlin to Harding line, causing it to sag and short on a tree limb. The Hanna failure caused wild swings of rerouted power as the grid strained to absorb the failures, but after interconnects with American Electric Power Co. failed power lines and power plants around the Northeast tripped off causing the regional blackout (PSERC 2003). The effect of the blackout can be dramatically seen in satellite images of the Northeast before and during the blackout (Figure 1).



Aug 13th Satellite Image of Northeast US and Canada. (Source: Platts Inc.)

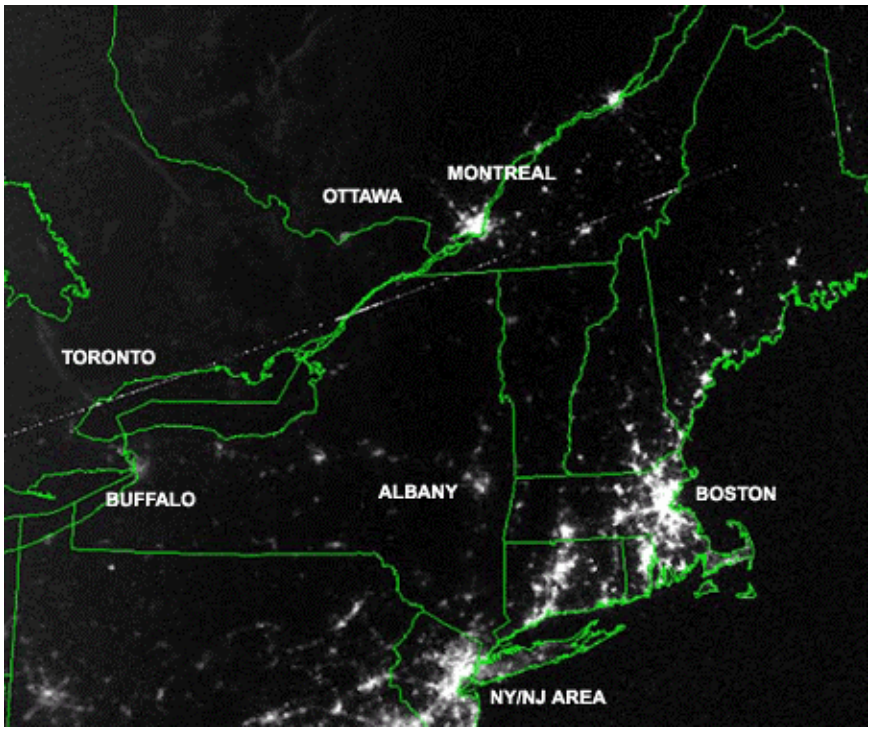


Figure 1: Satellite Images Prior to and During Blackout (Source: Platts Inc.)

The 2003 blackout also poignantly illustrated the interdependencies between the US's power network and Internet infrastructure. As power failed many regional and enterprise networks experienced outages, although most national backbone networks had adequate backup power supplies to survive the outage (Renesys 2003). The scope of network outages can be clearly seen in the figure below illustrating Internet routing outages during the blackout:

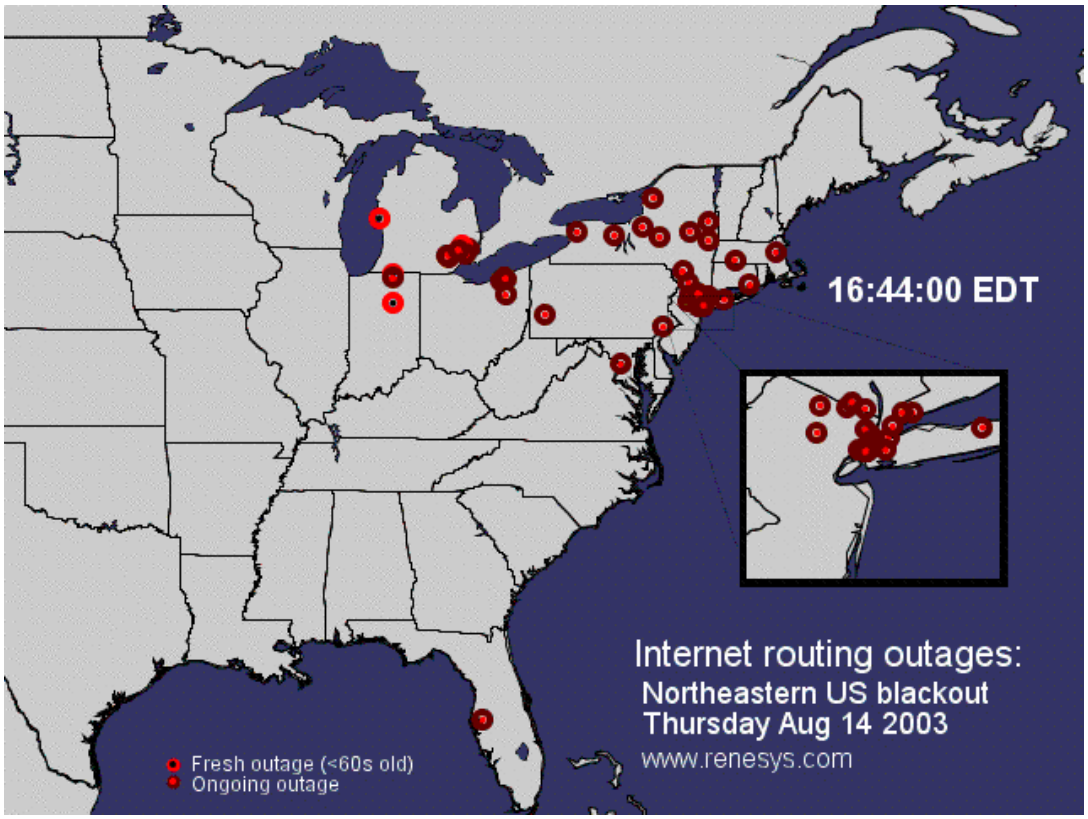


Figure 2. Internet Routing Outages During the 2003 Blackout (Source: Renesys Inc.)

While the majority has pointed to faults in First energy's power grid as the cause of the August blackout it has not escaped the scrutiny of conspiracy theorists connecting it to Al Queda. Coincidental evidence, like Egypt having the same SCADA vendor as the systems involved in the blackout and North American Electric Reliability Council (NERC) files suggesting a January 2003 cyber attack was a dry run on the power grid, has been used to make a weak case for terrorist involvement (Wilson 2003). More sound evidence of power grid sabotage was revealed in the FBI's arrest of a man in Sacramento, CA for dismantling 10 power grid towers through the Western United States (Lerten 2003). The arrested man claims he carried out the acts to point out vulnerabilities in the network.

Hollywood Cyber Attacks

The public perception of cyber attacks often takes its lead from Hollywood's imagination, "doomsday scenarios in which terrorists hijack nuclear weapons, airliners, or military computers from halfway around the world (Green 2002)." While perception can outpace even Hollywood the pantheon of real world cyber attacks often matches the movies in imagination if not impact. Cyber attacks have become increasingly sophisticated and the motivations behind them are often not juvenile hackers but organized crime syndicates and nation state actors. Tracking cyber attacks and discovering the culprits is incredibly difficult and rare, but the few successes and best guesses expose some disturbing trends. The following brief case studies are intended to illustrate the sophistication of attacks, their economic motivations, and possible implications for national security.

Millions of packets flood through a data pipe into a major Manhattan bank crashing upon the firewall acting as the bank's first line of defense. The tidal wave of packets overwhelms the firewall's ability to sort the traffic shutting it down and denying any traffic entry to the bank network. The attack causes a temporary network outage but on the surface has not violated the security of the network. Hidden in the flood of packets that saturated the firewall was a packet sniffer, that acts as a traffic spy gathering data unbeknownst to the network administrator. When the network administrator goes to reinitialize the downed firewall the packet sniffer grabs his/her user name and password and passes it along to the bank's unknown assailants. Money is then withdrawn from the compromised bank and sent to a second bank, and then sent to a third or fourth bank. By the time the breach has been discovered (typically a two hour window of operation) the money has been withdrawn from the final bank and the transfer from the intervening bank is a valid transaction. Only the intervening bank and originating bank created and authorized the fraudulent transfer and the terminating bank is not held liable. The monetary loss is covered by insurance and the system continues to operate. "Successful and unsuccessful attacks like one just described happen on a daily basis throughout the financial community[1]." according to one veteran security executive. The majority of cyber bank attacks are tightly covered from public attention by strict non-disclosure agreements in the name maintaining public confidence.

The Russian Connection

While the above incident comes from an undisclosed source and cannot be verified, there are growing public accounts of cyber attacks, which are increasingly linked with Russian organized crime. The growing problem of Russian cybercrime and the resulting financial loss led the FBI (2001) to issue a public warning about, "organized hacker groups from Eastern Europe, specifically Russia and the Ukraine" exploiting Microsoft vulnerabilities for financial gain. Russian organized crime has been documented by various media outlets to be responsible for a stream of high profile cyber attacks:

[1] Discussions with a security executive who requested anonymity, April 5, 2003

> …stealing secret Microsoft source codes, ransacking the Pentagon's computers, hacking into NATO's military websites, posting thousands of credit card numbers on the Internet, and stealing million of dollars from Western banks (Lunev 2002 p.1).

Specifics that outline targets and actors in cyberattacks are often difficult to come by. The few cases that have been prosecuted do offer insight into the nature of these operations. In 2001 the FBI arrested two Russian hackers by tricking them into coming to the United States for job interviews with security firms and hacking into their computers for evidence. While the Russian government protested the tactics employed by the FBI, the two hackers were tried and convicted in US court. The court cases revealed some interesting details of the hackers' methods and targets. The Russian pair first hacked into CTS Network services to launch attacks on two credit card processing centers, Sterling Microsystems and Transmark, while also stealing financial data from Los Angeles based NaraBank and FSI Inc. The second part of their strategy was breaking into Glen Rock Financial Service then threatening the exposure of credit card information if the company did not pay a ransom (DOJ 2002). Hack and extortion techniques have been a frequent tactics employed by Russian organized crime, the most prominent being the theft of 300,000 credit cards from CD Universe, which were then held for ransom (Lunev 2001). Reports maintain that Moscow houses the Civil Hacker School, which is funded by Russian intelligence agencies and Russian crime syndicates to ensure a steady supply of cybercrime talent (Lunev 2001). This supposed investment in developing cyber manpower has apparently paid off in the increasing sophistication of cyber attacks.

The Week of Internet Predators

Possibly the best recent example of the growing weight and sophistication of cyber attacks on the Internet was the attack of multiple predators across the Internet in mid August 2003. The first attack was the Lovesan worm, which attacked Windows XP and Windows 2000 operating systems starting August 11th with an executable file that randomly turns off the affected computer. Three different mutations of the worms infected hundreds of thousands of computers. Lovesan was followed by the Nachi worm, which used the same exploit, but also affected Microsoft IIS 5.0 servers. In a twist the Nachi worm killed the Lovesan worm and patched the vulnerability that allowed the Lovesan worm to propagate. The negative externality of this was a tremendous amount of Internet traffic, which overwhelmed and shut down many networks, including the world's largest Intranet belonging to the US Navy and Marine Corp (Messmer 2003). The third of the deadly trio was the Sobig.F virus that propagates through Microsoft Windows e-mail. The address from which the e-mail arrives is spoofed with domain names associated with the end-user. If the attachment is downloaded it executes a program that tells the affected computer to download a program from 20 different servers located across the USA, Europe and Korea. The virus also has been recorded to open proxies on affected machines allowing them to be used as Spam (unsolicited bulk commercial email) gateways to the Internet. Finally the big three predators have spawned scavenger predators like the Dumaru virus which sends a spoofed email from

support@microsoft.com that says it has a patch for the Lovesan worm. The attachment leaves a backdoor into the affected computer allowing it to be remotely controlled.

The latest round of cyber attacks not only illustrates a higher level of sophistication than just hacking incidents; it also illustrates an increasing level of impact. Detailed analysis of the attacks has uncovered some disturbing implications. Peter Simpson, manager of ThreatLab at Clearswift, maintains that the Sobig virus was developed by organized crime syndicates to facilitate Spam scams (Sturgeon 2003). Viruses like Sobig leave backdoors or Trojan horses on computers that allow them to be remotely controlled at a later date. Most often these backdoors are used to send Spam so that the unsolicited mail cannot be filtered out as coming from known Spammer addresses. While Spam is annoying it hardly seems to constitute a high level threat of any sort. This conception is beginning to change, as more evidence is uncovered. One of the latest discoveries reveals the utilization of these backdoors in a sophisticated credit card fraud scheme again linked to the Russian underworld. Computers that have been remotely controlled by virus-enabled backdoors are linked in a ring, and each computer hosts a porn site for a few seconds before it is passed off to another site. The ring also rotates compromised computers to send Spam, directing surfers to the web sites (GRID 2003). The sites then swipe unsuspecting customers credit card numbers. A similar plot by a group of Polish hackers uses virus-enabled backdoors to route traffic through compromised computers so that cybercrime activities cannot be traced. They offer the service to Spammers, purveyors of Internet fraud, and other nefarious groups as a form of invisible hosting (McWilliams 2003). There is a growing black market for hijacked computers that can be used for everything from Spam to distributed denial of service techniques. This black market provides a growing resource that significantly changes the scale at which cyber attacks can be waged.

Are cyber attacks from organized crime syndicates a national security issue, do they constitute cyber terrorism? The cyber terrorism question is matter of definition, but a reasonable case can be made that organized crime does play a role in funding and equipping terrorist groups. The academic literature and news reports indicate a strong linkage between organized crime, cyber crime, and the funding and growth of terrorist groups (Bequai 2002, Philippsohn 2001, Furnell and Warren 1999, Lunev 2001). Many of the cyber attack techniques outlined above have been directly linked to funding terrorist groups, including spam/porn, credit card theft, identity fraud, and money laundering (Bequai 2002). There have also been reports of connections between Russian organized crime and Al Qaeda in the appropriation of weapons of mass destruction and the utilization of Al Qaeda operative in Russian apartment bombings (Lunev 2002, Getz 2001). While the majority of evidence comes from often-unverified news reports the existence of growing cyber attack capacity in Russian and other organized crime syndicates is without doubt. Further, the connection between these crime syndicates and terrorist organizations is well documented. At a minimum the growing rate of cyber attacks and related financial crime is funding terrorist groups and it would not be a far leap to believe terrorist groups are considering evolving cyber attack tactics to aid their own missions. Both aspects point to cybersecurity as an area of increasing importance to national security.

Al Qaeda as a Cyber Threat

The analysis so far has examined critical infrastructure and cybersecurity as the focus of a general security threat with circumstantial connections to terrorism. The vulnerability of critical infrastructure is well documented from actual failures and the sophistication of growing malicious cyber attacks has been laid out, but are these areas that Al Qaeda are looking to exploit. Al Qaeda's connection to the technical skills to implement infrastructure attacks appear to be in place, but as stated before no terrorist has ever used a computer to kill a person. Further, Al Qaeda and other terrorist groups have always used physical attacks focused on inflicting the loss of human life to force world attention to their causes. Without precedent, is their evidence that is compelling enough to take serious precaution against a cyber threat that has yet to have occured?

A good place to start is by examining Al Qaeda's own rhetoric on the matter. On December 27, 2001 Osama Bin Laden put out a statement that, "It is very important to concentrate on hitting the US economy through all possible means (Verton 2003 p. xv)." This statement has become a mantra within Al Qaeda to focus on striking the "key pillars" of the US economy. Quoting this communiqué by Bin Laden, Al Qaeda's Abu Hafs Brigade claimed responsibility for the August 2003 Northeast blackout (Al-Hayat 2003). While post black out analysis and statements by the Bush administration ruled out any terrorist involvement in the blackout, the statement does make clear the attention Al Qaeda has focused on critical infrastructures and the US economy's dependence on them. The Al Qaeda statement went on to state that the goal of the supposed blackout attack was:

> hitting the major pillar of the U.S. economy (the Stock Exchange). [and] the UN, which is opposed to Islam, and is based in New York. It is a message to all the investors that the U.S. is no longer a safe country for their money, knowing that the U.S. economy greatly relies on the trust of the investor (Al-Hayat 2003, page 2).

While the statement was most likely opportunist propaganda it does point to an evolution in the strategies and tactics of Al Qaeda. It appears that Al Qaeda has come to believe that targeting the US economy can have a large damaging effect. Further, that the US economy's reliance on vulnerable critical infrastructures makes these easy targets. Last, that guerilla attacks and tactics on these infrastructures will erode public confidence having a devastating long-term impact on the US economy. Statements by Al Qaeda paint critical infrastructure as a strategic target but does Al Qaeda intend to use cyber tactics for possible attacks. In an interview with Dan Verton (2003) Sheikh Omar Bakri Muhammad, the leader of Al Qaeada connected al-Muhajirun stated that, "In a matter of time, you will see attacks on the stock market (p.84)." Bakri expands this statement by outlining how such an attack might go forward and how resources are being developed to do so," I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies. There are millions of

Muslims around the world involved in hacking the Pentagon and Israeli government sites (p.84)." Finally, the Sheikh concludes his statement with,

> I would advise those who doubt Al Qaeda's interest in cyber weapons to take Osama Bin Laden very seriously. The third letter from Osama Bin Laden a few months ago was clearly addressing using the technology in order to destroy the economy of capitalist states (p.85).

While the statements of Sheikh Bakri are definitive, it is suspect as to how much of the statement is inflammatory rhetoric to promote Al Qaeda's cause and how much is actual threat. According to special report on Internet Security by *The Economist* (2003) American intelligence uncovered an Al Qaeda hide out in Pakistan that had been used to train hackers to attack the computer systems of power grids, dams and nuclear plants. While none of this is a smoking gun it does point to a growing threat that US policy would be ill advised not to prepare for.

Cyber Warfare and the Nation State

Perhaps an even stronger argument for including both cybersecurity and critical infrastructure as integral aspects of national security is the growing cyber warfare threat posed by nation states. Conservative reports indicate that 20 to 30 countries are developing or already possess cyber warfare capabilities (Vegh 2002). The growing dependence of nation states on information technology for economic viability and military capabilities, have led to grandiose statement like:

> …cyberspace has become a new international battlefield. Whereas military victories used to be won through physical confrontation of weapons and soldiers, the information warfare being waged today involves computer sabotage by hackers acting on the behalf of private interests of governments (Adams 2001, page 98).

Cyber warfare itself dates back to the cold war, when Sandia laboratories traced virus attacks on US computers to originate from Bulgaria and East Germany (Guttman and Elburg 2002). Malicious attacks against Department of Defense computers have risen from 225 in 1994 to 40,000 in 2001 (Vengh 2002). Perhaps the most wide spread and damaging attacks occurred in march of 1998 and code named "Moonlight Maze" resulting in the theft of, " thousands of files containing technical research, contracts, encryption techniques, and unclassified but essential data relating to the Pentagon's war-planning systems (Adams 2001, p.99)." Red-teaming exercises that tested the strength US computer defenses like "Eligible Receiver" and "Zenith Star" both illuminated several vulnerabilities including the ability to shut off the power grids of nine cities, control the 911 emergency systems, and "paralyze" military command and control systems (Adams 2001). Many skeptics point out that there has been no hard evidence of foreign government involvement in any cyber attack (Vengh 2002). The ability to mask the origination of an attack makes the possibility of ever producing hard evidence

dubious, but there are other avenues to investigate the role of nation states in cyber attacks.

China's Cyber Soldiers

The most well documented cyber warfare initiative belongs to China's, which has been conducting cyber warfare exercises since 1997 and operating an information warfare military unit since 2000 (McDonald 2003). The ability to wage cyber warfare with information technologies is considered to be critical components of China's national strength (Yoshihara 2001). The growth and reach of China's information warfare capabilities is impressive, including the establishment of a cyber warfare complex in Bejucal, Cuba to monitor data traffic and intercept US communications (McDonald 2003). Security experts state that Chinese hackers are probing and mapping critical US systems, especially financial networks on a daily basis[2]. The gravity of these capabilities becomes more disturbing when placed in the context of Chinese military strategy documents. The release of *Unrestricted Warfare* provides an interesting perspective on the development of China's cyber warfare capabilities. The document proposes tactics for developing countries, in particular China, to compensate for their military inferiority vis-à-vis the United States during a high-tech war (Liang and Xiangsui 1999). The document reveals a strategy of asymmetric warfare that uses non-traditional tactics to defeat a military superior foe (explicitly the US):

> As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet, all can be included in the ranks of new-concept weapons (Liang and Xiangsui 1999, page 44).
>
> …in the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker (Liang and Xiangsui 1999, page 47).

While few would argue in current times that a hacker of even the most sophisticated cyber warfare capabilities match the threat of a nuclear weapon, it is clear that elements of the Chinese military see it as the future and are investing heavily in that future.

Investment in cyber capabilities may not well be confined to military expenditures. Since the telecommunications collapse of 2001 Chinese buyers have purchased PSINet, Level 3, Asia Global Crossing, and Global Crossing Inc., a total original US investment of $20 billion purchased for 3 cents on the dollar by various Chinese interests (Fonow 2003). Robert Fonow of the National Defense University (2003) believes these Chinese acquisitions could provide a platform for espionage and network warfare, citing that 95% of Department of Defense traffic uses the international telecommunications system. With the Chinese telecom acquisitions listed above most military and diplomatic traffic would pass over Chinese owned networks with some traffic passing through facilities in the Chinese mainland (Fonow 2003). The over riding

[2] Discussions a with security executive who requested anonymity, April 5, 2003

belief is that China plans to use its cyber warfare capabilities to prevent the projection of US force by preventing command and control apparatuses that guarantee supply lines and troop coordination (Fonow 2003). In fact may of these same tactics were employed by the US military in the invasion of Iraq to render the enemy immobile with a high level of success. A combination of such tactics in conjunction with disruptions of the domestic financial system paints a bleak if hypothetical picture.

Analysis

Greene (2002) in his *Washington Monthly* article is correct that terrorists cannot kill people with computers and further that no one has been killed by hacking or even cyber warfare incidents. Just because lapses in cybersecurity have not resulted in bloodshed, should not prevent it from being an issue of importance to national security. Terrorists have not used nuclear weapons to kill anyone either, but that does prevent the possibility from being a topic of grave concern. Greene and other do make a valid point that the hype and hyperbole of threat and reality do need to be investigated analytically. This short synopsis of catalogued events and evidence is an attempt to lay out what cases have been documented and what directions current trends could realistically take. Critical information infrastructure has two fundamental components, the physical fiber and devices and the data and systems that run over them, roughly broken in physical and cyber. Physical infrastructure is the less studied of the two but the impacts of random and planned failures exhibit significant impacts of areas diverse as financial systems and air traffic control. While there is a consensus that physical failures can have very damaging results there is little understanding of what parts of the infrastructure are most vulnerable or how to quantify what needs to be protected and the cost justification.

The area of cyber vulnerabilities is better documented and has many more cases of actual exploitation but also lacks thorough analysis of protection strategies and cost benefit analysis, especially in the realm of policy. The growing sophistication of cyber attacks points to a rapidly growing threat that has moved beyond simple web defacements and the motivations of teenagers hacking for fun. There is mounting evidence of cyber attacks being orchestrated by organized crime syndicates with documented connections to terrorist organizations. Further, there is growing evidence of nation states becoming heavily involved in developing cyber attack capabilities. The nature of both threats points to a fundamental understanding of information infrastructure as an area of critical national security.

Jurisdiction of Critical Information Infrastructure

In the aftermath of 9/11 critical infrastructure protection came to the fore in the US government, and telecommunication and cybersecurity became one of the most immediately identifiable areas of focus. Currently the security of the nations telecommunications system, which is in vast part controlled by private interests, falls under several federal jursidictions. Unlike the financial sector there is not a firm regulatory body or framework when it comes to the security aspects of telecommunications. In general telecommunications falls under the FCC, but when it

comes to security the federal mandate becomes less clear. The Whitehouse's National Communication System (NCS) was created for coordinating and planning the telecommunications sector to support crises and disasters. This role has grown since the agency's inception in 1962 to include the security of telecommunications infrastructure, as well as the Internet. Under the Clinton administration the Whitehouse's Critical Infrastructure Protection Board was also formed to look after the security of the nation's core infrastructure including telecommunications and its former head, Richard Clarke, was the federal government's cybersecurity czar. Agencies such as the Federal Reserve Bank and Department of the Treasury and Justice have also become involved in telecommunications security when it is an integral part of their domains as in the case of financial services and their related networks.

The creation of the Department of Homeland Security has again changed this landscape somewhat. On March 1, 2003 the NCS moved into the new Department of Homeland Security under the Information Analysis and Infrastructure Protection (IAIP) Directorate. According the President's fiscal budget $4.2 billion will be spent on cybersecurity in 2003 and $4.5 billion has been requested to protect critical infrastructure (Dean 2002, Green 2002).

There is undeniable government action in the area, but the effectiveness of this effort remains hotly debated. The analysis presented in this paper makes a case that there is a growing threat and without direct action to match these growing threats to existing vulnerabilities the United States will be in a position where cyber assets could compromise national security.

Works Cited

Adams J, 2001, "Virtual defense" *Foreign Affairs* 80:3 p. 98-112

Al-Hayat MS, 2003, "Al Qaeda claims responsibility for power blackout in U.S.!" *Dar Al Hayat* August 18 - http://english.daralhayat.com/arab_news/08-2003/Article-20030818-14bdd659-c0a8-01ed-0079-6e1c903b7552/story.html

Bequai A, 2002, "White collar crime: A handmaiden of international tech terrorism" *Computers & Security* 21(6): 514-519

Berinato S, 2002, "The truth about cyberterrorism" *CIO Magazine* March 15 http://www.cio.com/archive/031502/truth.html

CIPB, 2002, *The National Strategy to Secure Cyberspace Washington, DC*: Whithouse Critical Infrastructure Protection Board - http://www.whitehouse.gov/pcipb/.

Dean J, 2002, "Report stresses management's role in boosting cybersecurity" http://www.govexec.com/dailyfed/0202/021402j1.htm

DOJ 2001, "Press Release" - http://www.usdoj.gov/usao/cac/pr2001/104.html

Economist, 2003, "Fighting the worms of mass destruction" *The Economist* November 26 http://www.economist.co.uk/science/displayStory.cfm?story_id=2246018

FBI 2001, "E-commerce Vulnerabilities" http://www.fbi.gov/pressrel/pressrel01/nipc030801.htm

FCC 2001, *Network Outage Reports* http://ftp.fcc.gov/oet/outage/

Fonow R, C, 2003, "Beyond the mainland: Chinese telecommunications expansion" *Defense Horizons* 29:1-8

Furnell SM, Warren MJ, 1999, "Computer hacking and cyber terrorism: The real threats in the new millennium" *Computers & Security* 18(1): 28-34

GAO, 2003, "Critical infrastructure protection: Efforts of the financial services sector to address cyber threats" *Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives* Washington DC: U.S. General Accounting Office http://www.gao.gov/new.items/d03173.pdf

Gertz B, 2001, "Al Qaeda appears to have links with Russian mafia" *Washington Times* September 27

Green J, 2002, “The Myth of Cyberterrorism” *The Washington Monthly* November http://www.washingtonmonthly.com/features/2001/0211.green.html

GRID 2003, “Grid Technology Used to Hijack PC’s” http://www.gridtoday.com/03/0721/101704.html

Guttman B, Elburg K, 2002, “Israel: Cyber terrorism” *Computer und Recht International* 5: 156-157

Haggett P, Chorley R, 1969, *Network Analysis in Geography*. (New York: St. Martins Press)

Halsne C, 2003, “North Sound 911 Service Repeatedly Targeted” *KIRO TV* http://www.kirotv.com/news/2601577/detail.html

Kane M, 2002, “U.S. vulnerable to data sneak attack” *CNET http://news.com.com/2100-1017-949605.html*

Lerten B, 2003, “Tower saboteur: I was only pointing out flaws” *The Bend Bugle* November 23 http://bend.com/news/ar_view^3Far_id^3D12260.htm

Liang Q, Xiangsui W, 1999, *Unrestricted Warfare* Beijing: PLA Literature and Arts Publishing House

Lindstron A, 2001, “Tunnel Vision?” *Broadbandweek.com* http://www.broadbandweek.com/news/010806/010806_news_fiber.htm

Lunev S, 2001, “‘Red Mafia' Operating in the U.S. – Helping Terrorists” http://www.newsmax.com/archives/articles/2001/9/28/90942.shtml

Maine PUC, 2003, “Docket Number 2002243” http://www.state.me.us/mpuc/misctranscripts/2002-243%20080503.htm

McDonald H, 2003, “Beijing spies a useful friend in Castro” *The Age* February 27 http://www.theage.com.au/articles/2003/02/26/1046064102910.html

McWilliams B, 2003, “Cloaking Device Made for Spammers” http://www.wired.com/news/infostructure/0,1377,60747,00.html

Messmer L, 2003, “Navy Marine Corps Intranet hit by Welchia worm” Network World Fusion, 08/19/03 http://www.nwfusion.com/news/2003/0819navy.html

Neuman P, 1991, “NY area fiber-optic telephone cable severed; extensive effects” *The Risk Digest* 10:75 http://catless.ncl.ac.uk/Risks/10.75.html#subj1

Neuman P, 2000, "Week-long outage after cable cut downs 11,000 phone lines" *The Risk Digest* 20:84 http://catless.ncl.ac.uk/Risks/20.84.html#subj6.1

Newman R, 2002, "Wall street worries" *U.S. News & World Reports* September, 23

NIST, 1995, *The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security* Washington DC: National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-11/titleona.html

NRC, 2002a, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* Washington DC: The National Academies Press

NRC, 2002b, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later Washington*, DC: National Academy Press

NSTAC, 2002, *Network Security/Vulnerability Assessments Task Force Report Washington, DC*: The President's National Security Telecommunications Advisory Committee http://www.ncs.gov/nstac/NSVATF-Report-(FINAL).htm

Philippsohn S, 2001, "Trends in cybercrime – An overview of current financial crimes on the Internet" *Computers & Security* 20(1): 53-69

Renesys, 2003, "Blackout Results in Widespread Network Outages" http://www.renesys.com/news/index.html

Sturgeon W, 2003, **"**Organised crime behind Sobig - virus expert" http://news.zdnet.co.uk/internet/security/0,39020375,39115886,00.htm

Vegh, S, 2002, "Hactivists or Cyverterrorists? The changing media discourse on hacking" *Firstmonday* 7:10 http://www.firstmonday.dk/issues/issue7_10/vegh/

Verton D, 2003, *Black Ice: The Invisible Threat of Cyber-Terrorism* New York, NY: McGraw-Hill Osborne Media

Wilson J, 2003, "Blackout: The conspiracy theory" *Popular Mechanics* 180 (11): 37-29

Yoshihara T, 2001, "Chinese information warfare: A phantom menace or emerging threat?" *Strategic Studies Institute* http://www.iwar.org.uk/iwar/resources/china/iw/chininfo.pdf