The Digital Underworld: Cyber Crime and Cyber Warfare

Evan Baun

Abstract: At the dawn of the 21st century one of mankind's most profound inventions, the internet, has come to be associated with most parts of humanity's everyday life. The amount of human traffic on the internet has made the security of individuals or groups very difficult to protect. With the forces of globalization at its strongest, the internet has been pushed on our most important transactions of wealth and information and has made it a potential battleground among global actors. Due to an initial design of the free flow of information and limited security, the internet is rife with national governments, militaries, organized crime syndicates and individuals with programming skills exploiting these weak spots for enrichment in many different areas of interest. These ideas are tough to grasp for many individual internet users, so this publication serves as a general overview to how and why the world suffers the covert actions of some.

Key Words: cyber crime, cyber war, botnet, virus worm, Critical Infrastructure, malware, crimeware, hacker

Introduction

The hot topic of the moment in the realm of international security is not a new one, but it is finally being brought into the mainstream after a number of high-profile incidents. Cyber Warfare is the threat of the future that has clandestinely been wreaking havoc behind the scenes for years now having been warned about for more than two decades. And if you are hearing about this only recently and are asking yourself why you haven't been hearing about this threat all along, well, that is kind of the point. In the cyber world, everything is covert. Whether it is the lonely hacker sitting at home writing a virus to release on the "World Wide Web" to impress his comrades on a chat board, or the Russian criminal organizations stealing your personal and banking information while you make Christmas purchases on websites that proclaim "secured transaction guaranteed", to the Stuxnet virus that crashed an

Iranian nuclear reactor facility with no trail to the creator; the cyber world is furtive. Governments have not overtly stressed the issue to the general populace over the years because they are heavily interested in using these techniques for their own security and information gathering. Private industry doesn't promote the fact that their security isn't exactly up to par because they want your business and would rather not pay to take their systems offline to improve them. Attention brings regulation, and many believe that regulation limits both business and strategic opportunities.

The world of the internet can generally be seen in different ways: as a free marketplace and source of information, or a battleground. The average civilian usually goes to their favourite web sites to get their news, check up with friends and see what's selling on EBay, but doesn't really know how it all works or what is going on. The internet is like a digital version of the "Wild West" in America during the periods of its western expansion; full of endless opportunity and wide open spaces, but a hardly rule of law to be seen for miles. You are the innocent bystander in the conflict between the cyber "gunslingers", and your bank account and identity may just be lost in the fray. Perhaps even the electricity where you may live can be taken down. By now you are probably clamouring "Why is no one trying to protect me from this?" Truthfully, there are plenty of people, groups and governments blowing the whistle on this for some time, but like with any new domain it takes a great deal of time to figure out how and what to do to solve the problems. What type of an attack could be considered an act of war? Is that type of action is simply cyber vandalism? Some of these attacks are very sinister and criminal, while others are simply individuals not aware of the consequences of their actions. Because of the great level of misunderstanding and anonymity that exists in the cyber world, the ability to overreact in a given situation is extremely high, hence the slow process. One such incident awoke much of the world to the dangers that exist in cyberspace and the problems built into the system. This was no rogue government or terrorist organization, but a 15 year old Canadian with the handle Mafiaboy.

Mafiaboy, or perhaps less commonly known as Michael Calce, was a typical 15 year old trying to make a name for himself in his community where he operates. But instead of this world being a school lunchroom or football pitch, it was in IRC (Internet Relay Chat) which is essentially just chat rooms for groups of people or one-on-one chat. Mafiaboy was already very skilled in hacking operations (started at age 6) and by this time had written many programs that had earned recognition for he and his group named TNT/Phorce (a Russian hackers' guild) throughout cyberspace. All these actions could be perceived as actions of a bored and innocent youngster with adept computer skills just playing around with friends, until the day of February 7th, 2000 that is,

when his project entitled Rivolta (Italian for uprising) was unleashed upon the internet; more specifically onto Yahoo! Inc (Calce and Silverman 2008, pg 108). Rivolta was a Distributed Denial of Service or DDoS attack[1] that in a matter of days had brought not only the website of Yahoo! offline, but also those of CNN, Amazon, EBay, E*Trade, and Dell to name a few. The estimates of the losses from this attack range anywhere from $7.5 million USD to $1.2 billion USD, with the high end to be more likely ("Prison Urged for Mafiaboy" 2001). In Michael's book that he released in 2006 he stated none of this was meant for the financial harm induced, but only to make a name for Mafiaboy and TNT/Phorce in his community.

This attack was simply the act of a young boy who didn't understand the repercussions of a few hundred lines of code. However, this incident should bring to your attention that if there are those like Mafiaboy doing this much damage relatively innocently, then there must be those who know full well what their actions incur and are using them daily to put our financial institutions, military, power grids and research and development (generally known as Critical Infrastructure) at risk. You would be quite right. It is no longer a secret that groups such as the Russian mafia, Chinese Triads and Japanese Yakuza have made it a point since the early 1990's to focus on cyber crime because of the amount of gain that can be made, with little fear of being caught, simply by employing a few hackers. Also with situations like the tensions between Russia and Estonia in 2007, when a massive DDoS attack brought down Estonia's highly internet based banking and government websites, the fact that nations have been heavily invested in these types of activities is also no longer a secret.

The United States has recently declared it's cyber command (USCYBERCOM) to be fully operational, China has done the same on the island of Hainan (and among its civilian and military populations), and Russia has created hacker schools in the city of Voronezh under the control of the Service of Special Communications and Information to name a few. England, France, Israel, North Korea and Iran also have some of the more skilled cyber units around the world. "The vast majority of the industrialized countries in the world have cyber-attack capabilities," said former Director of National Intelligence Admiral Mike McConnell (Clarke 2010, 64). Governments not only procure these abilities themselves, but will recruit the support of their skilled citizens when the time is needed for cyber action. With all of these different

[1] DDoS definition from searchsecurity.techtarget.com: A distributed denial-of-service attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

types of characters out looking to exploit the internet and its built-in weaknesses, exactly how is it done and who is doing it?

Inside Cyberspace: How is it Happening?

On June 27th, 1991 computer security expert Winn Schwartau testified to the Congressional Subcommittee on Technology and Competitiveness, Committee on Science, Space and Technology on the state of government and private sector internet security:

Government and commercial computer systems are so poorly protected today they can essentially be considered defenceless - an Electronic Pearl Harbor waiting to happen. As a result of inadequate security planning on the part of both the government and the private sector, the privacy of most Americans has virtually disappeared (Schwartau 1991)

This was back in 1991 and of course he was dismissed for overreacting to the situation, as many of the experts are now still. Back at this time much of the US' Critical Infrastructure, such as nuclear power plants for example, had been connected to the internet since the 1970s with out-dated SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems) operating them. Not only that, but there are companies and government agencies that have our personal information on their systems with internet connectability. More on this subject will be looked at a bit later, but if all these things were a problem in 1991, imagine now. Before delving too deep into this area, let's take a step back.

If you ask most people who created the internet, some might reply with the answer Al Gore. Well, unfortunately they are wrong, but not entirely. Al Gore was instrumental in bringing the internet to the general public with the Gore Bill in 1991, just not in creating the actual internet infrastructure. The internet has its origins in the 1960s as a response to the USSR and *Sputnik*. The US government was looking for ways toward technological dominance over the Soviets, hence the formation of the Advanced Research Projects Agency (ARPA, or known as DARPA today) in 1958. The main goal was to improve the US information sharing and communications with the ability to handle many flaws, which was initially done by connecting radar networks. The creation of packet switching by Paul Baran at the RAND Organization was the first piece leading to true connectability. Not long after came the formation of ARPANET, the internet's predecessor, which linked different nodes at government and university research labs. Originally, there were four computers on this network from four different universities: Stanford, UC Santa Barbara, UCLA and the University of Utah. From this, the TCP/IP protocol was invented by Robert

Kahn and Vinton Cerf and we have the basis of our modern internet. For a more involved look at this evolution, take a look at http://www.livinginternet.com/ for quite an interesting overview of the process.

This brings us back to the quote by Winn Schwartau: if the internet was already rife with possibilities for exploitation before it had become widely accessible by the general public, why was nothing done about it while it was still relatively small in size? Well, because that was just the way the internet was intended, as a free flow of information and true freedom. With the US government and US universities in charge, no one would dare regulate freedom. A famous quote by former Senator Ted Stevens from Alaska, who was on the Senate Commerce Committee when a bill for net neutrality that would ban the ISPs (Internet Service Providers) from charging extra for priority use of the internet, brings joy to the lives of internet aficionados. Senator Stevens was vehemently against it, but his testimony sums up the general government confusion on the issue when he said:

[...] They want to deliver vast amounts of information over the Internet. And again, the Internet is not something that you just dump something on. It's not a big truck. It's a series of tubes**.** And if you don't understand, those tubes can be filled and if they are filled, when you put your message in, it gets in line and it's going to be delayed by anyone that puts into that tube enormous amounts of material (Singel and Poulson 2006)

Of course this sounds completely nonsensical, and it makes you wonder why someone who doesn't completely grasp the internet is in charge of regulating it or not. It becomes clearer why most were falling asleep in Al Gore's testimonies in the 1990s and why they probably didn't grasp what Winn Schwartau and other cyber security experts were getting at.

Former US National Coordinator for Security, Infrastructure Protection and Counterterrorism under the Clinton and George W. Bush administrations, Richard A. Clarke, in his recent book *Cyber War: The Next Threat to National Security and What to do About it* lists five major vulnerabilities in the general design of the internet that if not addressed, these holes in internet security can never be fixed. The first is the Domain Name System (DNS). This, which Mr. Clarke refers to as the internet's 411 information operator, is what you find when you type your "http://www." link into the address bar in your browser which is then converted into a number a computer can recognize, such as 168.45.130.22 for example. A request is then sent to that address to view the page and a positive or negative response is given when you do or do not receive the web page. This request travels along the lines of ISPs both big and small around the world to the server that hosts the website. This system was not built with any security parameters in mind, so a hacker can simply attack the DNS,

change the information, and send you to a fake website where they can receive your information. Another option is for the hacker to intercept your request packet, and send it back to you without reaching its destination telling you the site isn't there, or just misdirect it anywhere and cause internet chaos. This may just seem like an inconvenience to you, but to a company expecting to get visitors and transactions from a website that can't be accessed, the losses can be astronomical. There is a nongovernmental international organization that is supposed to be a regulatory body for the DNS entitled ICANN, but unfortunately they are unable to agree on a secure alternative, which leads Richard to state: "ICANN demonstrates the second vulnerability of the internet, which is governance, or lack thereof. No one is really in charge" (Clarke 2010, 79).

Next is the Border Gateway Protocol (BGP), which is the method that ISPs use to rout packets searching for websites that they do not host to the proper ISP; so in essence going to a house and asking for Mr. White, but you are told that he in fact lives in another neighbourhood and that person sends you there. The BGP works on trust between the ISPs, believing that any time a message comes and says "the website you want is located at my address" is legitimate. However, this system could easily be hijacked by an insider at an ISP or an outsider hacking in, sending packets flying blindly around the internet or direct them to where the attackers desire (such as in a DDoS attack). Issue number three is that the internet is unencrypted. Almost all of the traffic across the internet is unfiltered and easy for anyone to read. Packet sniffers can be used to pull in all the information of the traffic on a network. Some websites have secure logins, but that does not exactly mean everything is secure. If the user has accidentally downloaded a keystroke logger from a suspicious e-mail or website, this login information can be recorded as well.

The fourth major issue is the proliferation of viruses. The internet allows for the free flow of information, but also that of malicious code such as viruses, worms, Trojan horses and general malware that exploit defects in programs on your computer. These can be transferred through downloads, websites, e-mails, CD-ROMs, flash drives or even just being connected to the internet. Even though ISPs and government entities are monitoring the flow of malware, the sharing of information between all parties involved is at times quite poor. ISPs generally do not inform end users or governments of this malware because a combination of privacy laws, the slowing of the internet connection and because of the costs in general. Regrettably, a successful cyber-attack could affect the ISPs much more financially than the above costs. Most government and military bodies are only required to protect their networks and perhaps those of Critical Infrastructure (which will be explained better in the next section) in the private sector which they rely on for continued functionality. These entities

usually aren't called in until it's too late and a cyber-attack or cyber-espionage has already been successful. The fifth and final vulnerability Mr. Clarke lists is the internet's general design. The internet is decentralized and vast in size, which was the original intention so to not be controlled by governments or any one power, but unfortunately this has given way to the vulnerable network we have today. The original intention of the 1960's university minds given the political atmosphere of the time was good at heart, but inopportunely not meant for what the internet does today with its many built-in liabilities in security and privacy.

The Protection of Critical Infrastructure

As mentioned earlier, much if not all of a country's services that are seen as vital to the running of a modern nation state are connected to the internet. Many within the governments and industries of the world would assure you this is not true, but it's simply not the case. The Iranian Natanz nuclear facility infected with the Stuxnet virus (Zetter 2010) and the US Department of Defence (DoD) secure network named SIPRNet infected with the Agent.bzt (Mills 2008) virus apparently are air gapped between normal and secured networks, but that wasn't enough to overcome the use of thumb drives by inside personnel (presumably accidentally) to transport the viruses that brought certain parts of the systems crashing down. The Stuxnet virus has already demonstrated the danger that malicious code, no matter what type of actor it is, can be extremely dangerous when sent into the Critical Infrastructure of a country. In the Iranian case, the virus disrupted the Microsoft Windows 7 operating system that interfaced with the Siemens SCADA structures controlling the nuclear cyclones used for enrichment. The malicious code would tell the system to randomly stop these cyclones and then speed them up, eventually causing catastrophic failure and physical destruction of the systems.

Stuxnet has been a wakeup call to nations of the world as the virus itself is a digital work of deviant art. The virus first showed up in Southeast Asia in 2009 having been discovered by antivirus companies such as Symantec; but the industry couldn't tell what the virus did and it had no side effects to users who had contracted it. The virus worked its way into Iran, constantly recording information on its progress through cyber space and reporting back to its creators. The code also allowed for Stuxnet to be altered along the way depending on what information the creators had received. No one doubts the amount of time, money and insider information that was necessary in order to allow the virus to do what it did; targeting the exact specific systems that Iran had in place. This leads experts to believe that a nation state or states needed to

be behind such an ambitious and specific target. Those assumptions keep looking increasingly correct, as a United States and Israeli link has emerged. *Wired Magazine's Threat Level Blog* experts have been tracking evidence that after working with Siemens on testing the integrity of their PCS 7, or Process Control System 7 for controlling nuclear turbines in 2008, the Idaho National Labs (a part of the US Department of Energy) "may have passed critical information to Israel about vulnerabilities in a system that controls Iran's enrichment plant at Natanz" (Zetter 2011). From here *Wired* reports that the Israeli's rebuilt the setup at their Dimona nuclear facility (which has been the site of a joint US-Israeli operation against the Iranians nuclear plans for 2 years) in order to test the malware. Of course no definitive evidence exists that this is the case, aside from the massive circumstantial collection that has been gathered by researchers, but it wouldn't be the first time Israel has been accused of cyber operations in the past with the destruction of a Syrian facility in 2007.

To give another example of attacks on Critical Infrastructure we turn back the clocks to 2003 and the Slammer and Blaster worms, and more specifically to the Ohio based energy company FirstEnergy Corp. The Slammer worm first hit the scene on January 25th, 2003 when internet monitoring groups started noticing an overall slowing in traffic around the world. The worm had propagated a denial of service against ISPs, causing this general slowdown. The attack was focused on an error in the Microsoft SQL Server, thus was not a huge problem for people with home PCs (as this is generally not necessary for home use), but greatly affected businesses such as FirstEnergy Corp's Davis-Besse nuclear facility in Oak Harbor, Ohio. Though the Slammer worm didn't do too much damage to the plant (as it had been offline while recovering from a near breach of radioactive material months before), it did manage to crash the facility's Safety Parameter Display System (SDPS) which "monitors the most crucial safety indicators at a plant, like coolant systems, core temperature sensors, and external radiation sensors" (Poulsen 2003) even if the plant is offline. Then an hour later another safety monitoring program crashed. The worm had gone through the facility's unclassified network through a contractor and then into the classified system using the SQL vulnerability (Microsoft actually fixed this 6 months earlier, but no one operating the facility knew) and crashed the safety monitors. Overall, these systems took over 4 hours each to get up and running again, leaving the nuclear reactor vulnerable.

In the SQL Slammer case, the real amount of damage done was minimal, but the vulnerability shown was maximal. The importance of demonstrating this case is in order to demonstrate the susceptibility of nuclear facilities such as the Davis-Besse one; and the vulnerability of FirstEnergy Corp. Then entered W32.Blaster, which was a worm that attacked Windows operating systems and hit the internet on August 11th, 2003. Soon after its release, a huge cascading

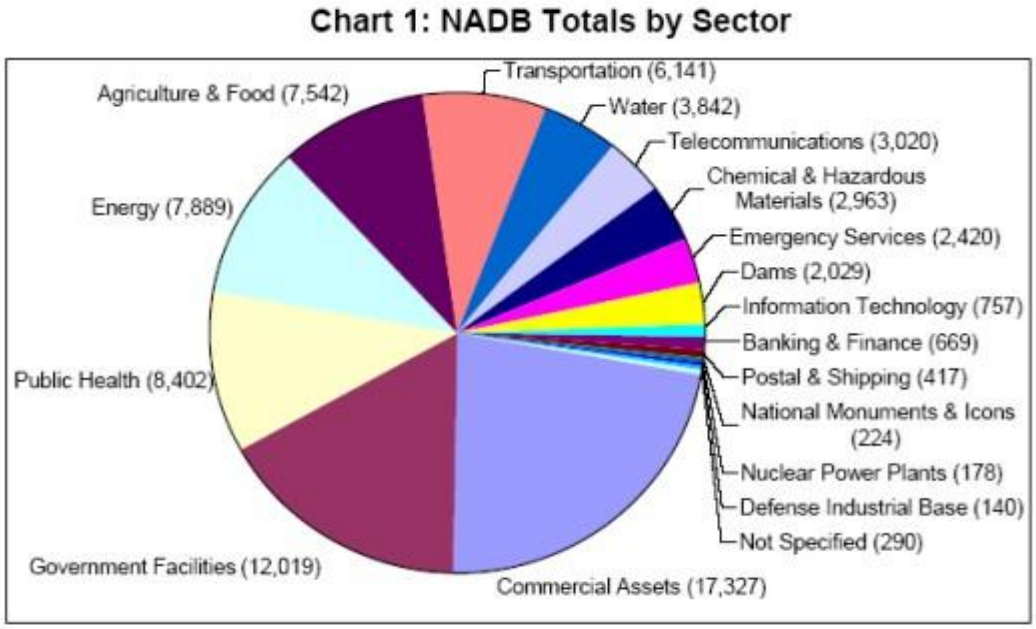
power failure in the Northeast United States and Ontario, Canada began and around 55 million people were living without power for days (depending on where), along with the disruption of telephone and water services to the tone of an estimated $10 billion lost ("Huge Threat to Power Grid" 2009). The power disruption was linked back to a surge in power lines in Ohio with supposed overgrowth of plant life to be the culprit. This very well might be true, but there are some more important aspects to look at here. Reports at first were that FirstEnergy's Eastlake facility operating and warning systems were working fine, even as power started failing all throughout the area. Typically the alarm systems would be activated in such an event, but it seems there was an error that had disabled these systems for over an hour. Following this came reports of frozen screens on the Windows operating systems from the operators themselves, all of which put significant delay into the discovery and correction of the problem. While it is true that Blaster may not have been the cause of the blackout in 2003, as the official report claimed it was not, looking at the facts it seems Blaster may have played a role in exacerbating the problem and delaying the response.

Fast forwarding to August 2005 we can see the effects of yet another worm proliferating DDoS attacks on yet another sector of infrastructure; the auto industry. Around this time the Zotob worm began to hit the internet. On August 18th, a total of 13 DaimlerChrysler auto plants were taken offline when Zotob entered the company network, and then quickly went into the control systems. Once in one of the company computers on the network, the virus easily spread to the other plants. The results of the Zotob worm were that 50,000 assembly line employees were unable to work and the losses were at around $14 million for only about an hour of lost work time (Roberts 2005). This example gives a great look at how a virus can cause even the smallest of effects on a company, yet the financial losses can be massive.

These were examples of viruses affecting Critical Infrastructure and big business without specifically meaning to do so (that we know of). Most likely these worms and their variants that propagated these DDoS attacks were simply floated out into the internet to see what they were capable of (much like Mafiaboy). But to get a better look at this type of an attack from a controlled environment, we look no further than the Idaho National Labs and Department of Homeland Security (DHS) test case of Aurora (Not to be confused with the cyber-attacks on Google by China named Operation Aurora). This controlled test took a $1 million electric generator from the Alaska power grid and hooked it up into a simulated network identical to those used by certain power companies. Then the lab had a hacker attack the system from the outside, and in a matter of time he had reached the computers controlling the SCADA systems and slowly the generator self-destructed (Meserve 2007). As more of

these types of obscure systems controlling much of industry's hardware are moving to well known, updated systems with greater connectablilty, the more easily this type of hack is to succeed on Critical Infrastructure.

The US government has issued two major studies recently to look at the state of their Critical Infrastructure: The Government Accountability Office (GAO) report in 2010 entitled *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed* and its predecessor the Congressional Research Service (CRS) report in 2007 entitled *Critical Infrastructure: The National Asset Database*. The latter report looked at around 77,000 entities addressed in the 2006 DHS Inspector General report thought to encompass Critical Infrastructure brought about by the 2003 DHS National Infrastructure Protection Plan (NIPP), which DHS claimed that through this number you can attain a list of 600 assets that are critical to the functioning of the United States. The reasoning behind this slimming down is because of those 77,000 assets many are malls, zoos, parks and other places that people congregate that are probably targets for a terrorist attack, but not really a cyber-attack. The chart below shows the sectors of critical assets to which DHS addressed to get a better look at what is viewed as critical to the nation. The same is probably true of most industrialized nations.



Source: Office of the Inspector General. Department of Homeland Security. Taken from
Progress in Developing the National Asset Database, pg 5.

The GAO report focused more on these assets and their cyber vulnerabilities, being asked to look at (1) private sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met and (2) public sector stakeholders' expectations for cyber-related, public-private partnerships and to what extent these expectations are being met (GAO 2010). Basically, the private stakeholders want good information of the high level/classified type on cyber threats and for the government to be less fractured in its approach to cyber security. The public sector wants similar action, specifically the private sectors' unwillingness to give sensitive information on cyber-attacks for fears of market losses and stolen proprietary information (which happens at an alarming rate anyway), and for the private sector to do a better job at adopting plans and recommendations for cyber protection. Needless to say, these studies show that the Critical Infrastructure is quite large in the United States and also that the public and private sectors are still quite disjointed when it comes to the protection of these assets; regardless of how many Presidential Directives are signed.

MacAfee Antivirus issued a study entitled *In the Crossfire: Critical Infrastructure in the Age of Cyberwar* in 2009 that surveyed 600 leaders in the field of cyber security that protect Critical Infrastructure worldwide. Many of the findings here, as with many of the studies in the field, are quite shocking. The findings of the study, explained by Brian Prince from eWeek.com, show:

- On average, monetary losses for down time of Critical Infrastructure systems of the group surveyed was $6.3 million per day, and $8.4 million per day for the oil and gas industry
- Only 19% implemented "whitelisted" technologies for SCADA/ICS and IT protection, despite these monetary losses
- Only 57% of executives overall said their organization patched and updated software on a regular schedule, with Russia and Australia leading the way with 77 and 73%, respectively. Brazil was at the bottom with 37%. Only 1/3 of security executives stated their company had a policy against the use of removable/thumb drives
- The most widely adopted security measure overall was the use of firewalls between private and public networks, which 77% reported using (65% for SCADA or ICS systems)
- Technologies such as security information event management (SIEM) and role and anomaly detection tools were deployed by 43% and 40%, respectively
- In virtually all cases, China led the way in adoption of security technologies. When IT and security executives were asked about 27 dif-

ferent security measures in the survey, China was found to have the highest security adoption rate, standing at 62%. That figure is roughly 10% higher than what was reported by the United States, Australia and the United Kingdom

- Overall, 54% of respondents said they have already suffered a large-scale denial-of-service attack by organized crime gangs, terrorists or nation-states. In addition, 37% of IT executives said the vulnerability of their sector had increased over the past 12 months (Prince 2010)

While these findings contain a lot of figures that can be intimidating to read through, as most security assessments can be, the proof is in the numbers: Critical Infrastructure across the world is not generally safe.

These vulnerabilities are certainly a hindrance to all the people trying to run financial sectors, governments or even households using the interconnectedness and ease of the web. The ability to exploit from all angles is only getting greater, and with rapid internet expansion all over the world to places such as Africa (which threatens to become the world's biggest botnet[2] one day) and because of the trend towards privatization of Critical Infrastructure over the years, new vulnerabilities and the scope of the battleground is only increasing. Now that the general scheme of the internet, connectedness of Critical Infrastructure and the susceptibilities of both are better understood, let's take a look at all the types of actors and the type of activities they are involved in within the online community.

Crime and Terrorism: The Cyber Underground

Did you ever wonder how truly interconnected the world is in this age of globalization? While presenting at the 2010 Concept Development & Engineering Conference (CD&E) in Norfolk, Virginia, the Regional Director for Security and IT solutions from Verizon Business, Brian Costello, presented recent estimates on the cyber state of the world. Verizon is one of the 6 major ISPs in the United States, and operates in 158 markets and 214 locations around

[2] Botnet definition from Microsoft.com: The term *bot* is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*.

the world, so they would have about as good an idea of these numbers than anyone:

- 20.2 Exabytes Global IP Traffic (2010 Forecast)
- 13.2 Million Fiber Miles Deployed (2009)
- 500 Million Facebook Users (Aug 10)
- 5.3 Trillion Text Messages (2009)
- 180 Million Global Smart Phones Shipped (2009) (Costello 2010)

Overall, that is a lot of information that a lot of people are sending across the internet. Not only personal but financial as well, and that's where cybercrime comes into play. People are now doing banking transactions over smart phones (with great vulnerabilities as well), buying gifts online on Amazon with credit cards and making important business decisions over e-mail. This means that there are even more ways for hackers and criminal organizations to steal your information, or even your identity. Let's take a look at the state of cybercrime in the world.

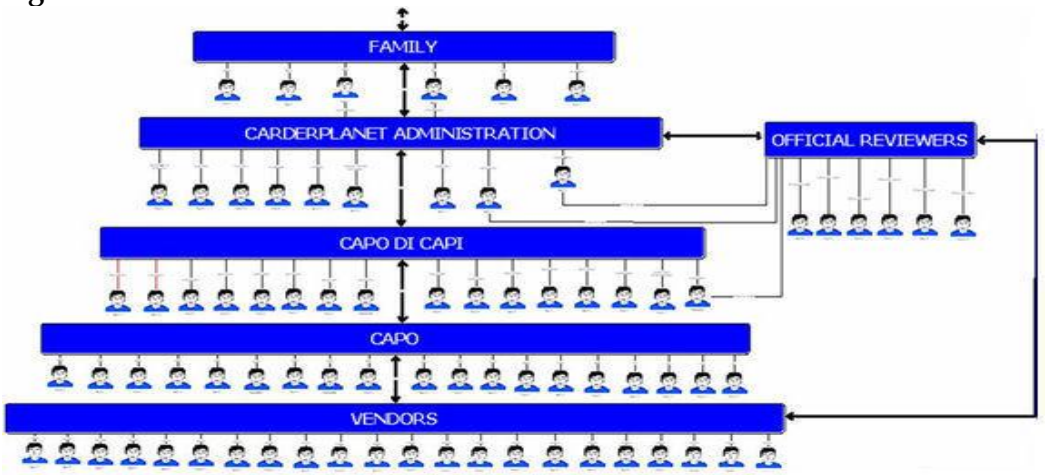
The United States Federal Bureau of Investigation (FBI) has officially listed cybercrime as the #3 priority of the organization. The FBI is the only American federal agency with the ability and mandate to deal with cybercrime in the country, as they specialise in the areas of computer intrusions, child pornography, internet fraud, cyber terrorism and so on. In order to have an effect on cybercrime, much of which is across borders, you need to have a global reach to be able to work with partner nations in order to bring these criminal gangs or individuals to justice; which the FBI has. At the 2010 CD&E Conference, FBI Assistant Special Agent in Charge Norfolk Division, Mr Willie Session, demonstrated the challenges that law enforcement in the United States faces:

- In 2009 the U.S. led all nations as the origin and target of cyber-attacks
- The Financial Sector was the victim in 74% of all cyber-attacks
- There were 336,655 Internet Crime Complaint Center complaints filed in 2009 which represented a $560 million economic loss
- Global hackers infiltrated 2500 corporate and government agency networks and stole personal and proprietary information (Session 2010)

Once again staggering numbers, but it's what happens given an insecure internet structure and almost every human being on the planet having at least some access, computer knowledge and a lack of solid financial and job opportunities.

The world of cyber-crime is starting to become more organized, and has begun to take on a mafia-like structure. For example, the Eastern European criminal organization CarderPlanet that was in existence from 2001 to 2004 was a mainly Russian language site where one could buy stolen credit card accounts. The site was forced to shut down after the arrest of some of the higher members of the organization, but from here many criminal groups were spawned across Europe. Figure 1 below from McAfee demonstrates the structure of CarderPlanet.

Figure 1: CarderPlanet Structure



Source: Paget, Francois. "Cybercrime Organizations Turn to 'Mafia-Style' Structure."
Taken from *McAfee Blog Central*

The types of specializations available in the cyber underground were laid out by Steven R. Chabinsky, FBI Assistant Director, Cyber Division, while speaking at the GovSec/FOSE Conference and Expo in March 2010 are as follows:

- **Coders or programmers:** who write the malware, exploits, and other tools necessary to commit the crime
- **Distributors or vendors:** who trade and sell stolen data, and act as vouchers of the goods provided by the other specialties
- **Techies:** who maintain the criminal infrastructure, including servers, bulletproof ISPs, and encryption; and who often have knowledge of common database languages and SQL servers of course

- **Hackers:** who search for and exploit application, system, and network vulnerabilities to gain administrator or payroll access
- **Fraudsters:** who create and deploy social engineering schemes, including phishing, spamming, and domain squatting
- **Hosters**: who provide "safe" hosting of illicit content servers and sites, often through elaborate botnet and proxy networks
- **Cashers:** who control drop accounts and provide those names and accounts to other criminals for a fee, and who also typically control full rings of our eighth category, money mules
- **Money mules:** who complete money transfers or wire transfers between bank accounts
- **Tellers:** who help with transferring and laundering illicit proceeds through digital currency services and between different world currencies
- **Leaders:** They're the "people-people." They choose the targets; choose the people they want to work each role; decide who does what, when, and where; and take care of personnel and payment issues. Many according to Chabinsky don't have any technical skills (Detwiler 2010)

There are many possibilities out there for people with certain talents, and all business is done behind closed firewalls and of course tax free, so the opportunities are there for these skilled individuals.

In a way, cyber-crime can be seen as the research and development sector for much of the spyware, viruses and hacks (aka crimeware) out there. In a capitalistic world, there usually needs to be some sort of monetary gain to induce the creation of the newest technologies, and the same is true with crimeware. Criminal gangs have been learning how to exploit every little thing they can on computer systems that control documentation and numbers. The web security firm Finjan pointed out trends in 2008 of criminal gangs exploiting vulnerabilities in Adobe programs (mostly Flash and Reader applications) in order to propagate their crimeware and get access to your information. These programs regularly update and most people don't think twice about clicking on an Adobe update, and this is what makes the exploit perfect. The amount of money available to groups by data phishing (pretending to be a credible source to receive sensitive information), carding (dealing of stolen credit and banking information) and identity theft (stealing of personal information and articles such as passport information to allow someone else to be you) to name a few are extremely profitable, especially in areas of the world where the government doesn't care about stopping such activities.

Even the searching out of these people is considered privately profitable, as companies such as Microsoft have put up a $250,000 bounty for anyone

giving information that leads to the arrest of people involved with the creation of viruses that exploit their systems (Neild 2009). In certain situations, which will be covered more in the next section, governments have no interest in stopping said criminals because these are the same individuals recruited behind the scenes for political hacktivism by state entities; so the two groups live off of each other and work together. In fact, most all the actions and tools used, along with the people, groups and state entities involved are the same whether you call it cyber-crime, cyber espionage, cyber terrorism or cyber warfare; but for the sake of this publication we will break everything down more individualistically and try to show the links between them throughout. The basic idea of cyber-crime is the same to that of regular organized crime. There are many groups perpetrating these types of crimes in areas of the world where the chances of their arrest are slim.

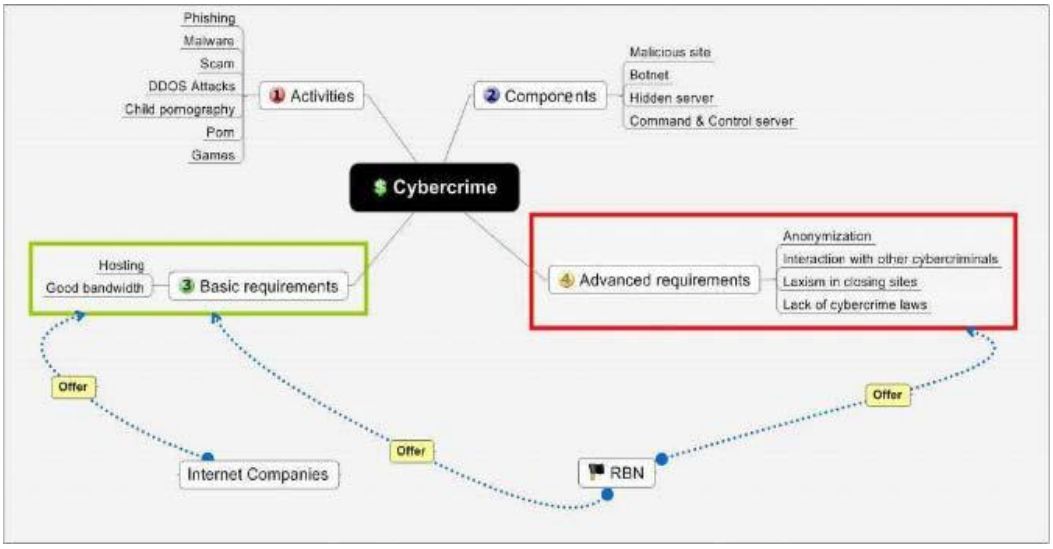
South American Groups

The continent is not the first place you would think of when the idea of cyber-attacks arise, but when the digital risk management firm mi2g listed the top 10 most active hacker groups of 2002, all were Brazilian. There is some speculation that the level of activity of Brazilian cyber criminals is due to the fact that Brazil won the World Cup that year, which is surely a point when addressing the level of activity, but mi2g's Chief Executive DK Matai has a different opinion for the overall numbers: "Brazil has a very well developed IT software capability and software outsourcing industry which European and US companies utilise. At the same time, Brazilian society has a fairly high level of crime which inevitably spills into cyberspace" ("Hackers Catch World Cup Fever" 2002). This is probably the same of most South American, Central American and Caribbean nations when it comes to relaxed cyber laws, banking laws, corruption and organized crime (such as the drug cartels). Apparently the groups are difficult to attribute directly because they change names and identifications so often, but it is believed to be a small and tight nit group based on the skill of the Trojans that come out from the area. Director of Threat Intelligence at the firm SecureWorks, Don Jackson, states of the skill of these hackers, specifically with their attacks on the banking sectors that "while Russia is good at financial fraud and credit carding and that type of thing, the South American Trojans are about automated man-in-the-middle, defeating-two-factor-authentication type attacks" (Chickowski 2008, pg 3). When it comes to financial sector hacking, these groups know how to do it and are constantly adapting.

Russian Business Network (RBN)

The RBN is perhaps the most famous entity in the cyber world when it comes to hacking and organized crime. Although the organization does not exist with the same label RBN as it did when founded in 2004, it is easier for people to use the title when referring to this entity of Russian/Ukrainian/Belorussian bulletproof hosting for criminal organizations and their botnets. The organization started off as a legitimate hosting site, but found out it was more profitable to host illegal services and organizations. The groups using the RBN would use phishing attacks by e-mail to steal individuals' information by tricking them into entering personal and banking info into fake sites. *The Washington Post's* Brian Krebs, whom runs the *Security Fix* section on computer security, reveals in his article *Mapping the Russian Business Network* the major internet providers whom allow the RBN their connectivity and names the firms as follows: Tiscali.uk, SBT Telecom, Aki Mon Telecom and Nevacon LTD (Krebs 2007). This doesn't mean that these firms directly knew they were supplying the internet connections for this criminal organization, but not enough research was done into their clients to do something about their cyber activities. Brian Krebs' reporting of work done by cyber researchers such as James McQuaid and Jart Armin helped expose some of the organizations knowingly aiding the RBN such as the California based Atrivo/Intercage, and other such hosts like Estonia's ESTDomains and Russia's McColo (both of which were heavily linked to the US and US firms) (Carr 2010, 125-28). Krebs received threats for his work in exposing these organizations.
The RBN is responsible for most of the advancement of worms and other viruses that steal personal information during the 2000s, and some of the most notable listed by Krebs are malware such as Gozi, Grab, Haxdoor, Metaphisher, Mpack, Ordergun, Pinch, Rustock, Snatch, Torpig, and URsnif. They have also been accused of having political connections. The RBN's top man who goes by the handle Flyman is responsible for many of the criminal connections of the organization and is said to be the nephew of a prominent Russian politician (Warren 2007). Accusations have also been made with the group being involved with the cyber-attacks on Georgia and Azerbaijan in 2008. The graph below is a layout of how the RBN has worked.

Figure 2: Russian Business Network Layout



Source: Carr, Jeffrey. *Inside Cyber Warfare*. Pg 124.

WikiLeaks, Anonymous & LulzSec

Some groups of hackers are not in the game for purely monetary gain; some are in the game for political and social reasons. Whether for anarchical desires of chaos or rogue righteous vigilante justice on some perceived wrongdoing, these groups use their hacking expertise to run the gamut of attacks on various targets for various goals beyond stealing credit card numbers. The most famous (or infamous) of these groups has become WikiLeaks and their enigmatic front man Julian Assange. Though WikiLeaks is not exactly a hacker group but a non-profit forum for the posting of classified information, most nations and companies see no difference if they are the ones posting the info or stealing it. WikiLeaks, and specifically Assange himself, has become target number one by nation states whose secret to top secret information has been obtained and published by the group. The largest of said leaks, originally copied from US military networks by US Army Intelligence Analyst PFC Bradley Manning, have been released throughout 2010-11 and revealed many of the inner workings and secrets of the United States in regard to the wars in Afghanistan and Iraq, as well as decades' worth of diplomatic cables and eventually information on the Guantanamo Bay internment facility (Poulsen and Zitter, 2010). This leak was composed of some hundreds of thousands of documents, and while the information is very damning of the United States on many fronts, much of the

information is not particularly shocking for most experts to hear that these types of things were being done or said during these periods of war. Some of the news, such as with Abu Ghraib, had been uncovered previously in detail. As a result of subsequent attempts to shut down WikiLeaks, along with companies such as VISA, Mastercard and PayPal disallowing their services to the group and removing their main source of funding, likeminded groups such as Anonymous set their sights on the government and corporations' websites. The aptly named "Operation Payback" succeeded in taking down these sites for a period by DDoS attack for their perceived wrongdoings against WikiLeaks (Hall and Winter 2010). Groups like WikiLeaks nonetheless believe that these types of information are pertinent and need to see the light of day, and they have many others out in the cyber universe who identify with this stance.

Anonymous is a decentralized hacktivism group that is run out of websites and forums such as 4chan, IRC and Futaba. The group has existed since 2003 and counts its members as a collection of random like-minded vigilante hackers. Anonymous has gone after the websites of all types of groups ranging from specific cities, political parties, churches, copycats, and even Middle Eastern governments and leaders during the period of the Arab Spring in 2011. Anyone that has done a supposed wrong to the group or to people in general is fair game for the group. Obviously they are much looser knit than cyber-crime gangs, but due to the activity in their forums they are able to mobilize a group of hackers quickly and for a specific purpose. More recently with the rise of movements against unfairness and inequality around the globe such as Occupy Wall Street, Anonymous has begun to step up their attacks towards big banks and their leaders. A recent hack of the International Monetary Fund (IMF) along with threats against the US Federal Reserve and its chairman Ben Bernanke with quotes like "End the campaign finance and lobbying racket, Break up the Fed & Too Big to Fail banks, Enforce RICO laws against organized criminal class, Order Ben Bernanke to step down" on the same day have let the US government know they are serious (Comstock 2011a). A recent US Department of Homeland Security report has noted that the group Anonymous has begun to also show interest in the hacking of Critical Infrastructure. DHS has stated "the information available on Anonymous suggests they currently have a limited ability to conduct attacks targeting [industrial control systems], however, experienced and skilled members of Anonymous in hacking could be able to develop capabilities to gain access and trespass on control system networks very quickly" (Zetter 2011). It is unknown if this is truly a desire of Anonymous or simply speculation, as so far they have not been known to target these types of systems for destructive purposes. Even though the report shows the group has been active in working through these systems and searching for the types of equipment that Stuxnet would be

interested in, DHS does not see an immediate threat. Since Anonymous has recently joined forces in the battle against "too big to fail banks" with another hacking group LulzSec, the threat is being taken more seriously (Comstock 2011b).

LulzSec (Lulz Security) is a hacker guild believed to have been started in May 2011 with the explicit goal of causing mayhem for entertainment, or for the "lulz" or laughs. The group "claims to be exposing security vulnerabilities in websites and organisations purely for "fun". But their willingness to dump the stolen data and details they uncover online pushes them towards the black hats" (Taylor 2011). LulzSec has claimed responsibility for a variety of hacks in 2011 that have ranged from the CIA, the governments of Brazil and Arizona, as well as Sony Pictures and News Corporation. Information on the six or so members of the group have been leaked to *The Guardian* by other hackers and even by the members themselves; leading to a few arrests of supposed members. The largest undertaking by the hacking group to date has been named "Operation AntiSec". The operation promotes the hacking of various websites, generally government and banking, with the desire to deface them with the script "AntiSec". LulzSec states that with "Operation Antisec" its "top priority is to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments" (Ross 2011). As mentioned earlier LulzSec has joined with Anonymous to take on some of these tasks, but is in a state of flux with the arrest of prominent members.

Cyber Warfare: State Weapons of Mass Destruction or Mass Annoyance?

Its becoming more and more clear that the internet is not only the backbone of information sharing in the world's new globalized information market, but also another realm of existence that is just as dangerous as real life can be. Not only are nations using it as the new 21st century battlefield, but even ordinary citizens with a certain level of computer skills are capable of jumping in and inflicting mass amounts of damage. The threats that are constantly brought up by internet watchdog and security groups about how countries like Russia, China and the United States can bring down power grids, banking sectors and water purification plants not only rest in the hands of nation states. Civilian groups are also becoming increasingly more sophisticated in these areas and are at times extremely difficult to locate and arrest. With all the vulnerabilities that exist within the internet itself, like the ones mentioned earlier by Richard Clarke, action needs to be taken to secure the web.

For nations, cyber actions such as those incurred by Estonia in 2007 could possibly lead to physical conflict or war in the near future. The line between cyber espionage and cyber war is extremely blurred and perhaps presently benefit most countries with the way things are. In the case of attribution many states cannot follow the attacker because of international agreements between nations, and a server may physically lie in an unwelcoming nation. Countries like China and Russia are not likely to agree on international legislation to calm cyber espionage as the current situation serves them to such a large extent in their development and security in many areas. The same can be said for the US and EU, as well as nations like Israel and Iran and organizations like NATO, but there will come a point when the level of cyber activity by these states against each other could drive the world to the brink of war. What if it is not only security services of nations stealing each other's information, but private companies of one nation stealing the proprietary information of another? Would this event incur the same wrath from nations as well?

The next Stuxnet attack could be the straw that breaks the camel's back. So, would cyber-arms limitation treaties that resemble what were done with nuclear weapons during the Cold War be the way to go? Perhaps this will be the case. Maybe the best way would to try and solidify the weak points in the internet that lead to the extraction of information and financial data all over the world. All of these steps will probably be in play in the future, but for now best way to address these fears for nations in the short term would be to shore up their own government, military and private sector cyber security. By creating separate internets that are off the grid for important national information, along with securing Critical Infrastructure that cannot be communicated with or operated from abroad, the security situation can improve. Of course this doesn't take into account the biggest chance of error of all: humans. Unfortunately humanity is one variable that will be the hardest to remove from the equation, such as military intelligence officers like Bradley Manning with access to military intelligence and computer skills to boot. Training and awareness of certain scenarios by organizations can help remove part of the problem.

Another way to improve security, surprisingly enough, is greater communication. The more that government interacts with critical private industry and work together on countering threats, the better. The same goes for nations, specifically those in an Alliance such as NATO. Each country in NATO has certain sensibilities about letting even their partner nations know certain things about their networks, but the more information sharing between allies can lead to foiled cross border cyber-attacks. For example, many of the attacks on Estonia in 2007 were wired through Germany, even though the Germans

weren't attacking Estonia. Greater collaboration between the nations could allow Germany in this case to be more proactive when their monitors notice an uptick in activity aimed at Estonia from a third party nation, and increase attribution assurance. When it comes to cyber-crime, the same type of collaboration could put a real dent in cyber operations. If regional police or a federal agency notices some activity, or knows that an attack could be operated from their area and can quickly interact with INTERPOL to cut off an operation before it can steal enormous amounts of money and inflict major damage, nations would be beneficiaries as well. Collaboration at all levels is the best way of thwarting cyber espionage, terrorism, crime and warfare.

So, what does the future entail in cyber space? For the time being it looks like much of the same. For every programmer sitting in an office writing code for a new network firewall to sort out the good from bad traffic, there is another programmer somewhere figuring out how to break through just so he or she can brag about it, and maybe turn a pretty penny. Just exchange the words "office" and "USCYBERCOM" and the breadth of the problem presents itself. The internet is surely one of humanity's greatest achievements, but can also be designated one of its greatest weapons just as easily, and just about anyone with a little skill can trigger it.

Bibliography:

Calce, Michael and Craig Silverman. *Mafiaboy: How I Cracked the Internet and why it's Still Broken. Toronto: The Penguin Group, 2008.*

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, Inc., 2010.

Chickowski, Ericka. "Inside Online Crime: Of Hackers, Identity Theft and Online Scams." *Baseline*, August 22, 2008.

http://www.baselinemag.com/c/a/Security/Inside-Online-Crime-Of-Hackers-Identity-Theft-and-Online-Scams/2/ (accessed January 15, 2011).

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to do About it*. New York: Harper Collins. 2010.

Comstock, Courtney. "Anonymous: Bernanke is Next." *Business Insider*, June 12, 2011.

http://www.businessinsider.com/anonymous-bernanke-is-next-june-14-2011-6 (accessed October 15, 2011a).

Comstock, Courtney. "Hacker Group Anonymous Teams With LulzSec To Declare War On Too Big To Fail Banks." *Business Insider*, June 20, 2011.

http://articles.businessinsider.com/2011-06-20/wall_street/30078377_1_top-priority-whitehat-banks (accessed October 20, 2011b).

Costello, Brian. "The Cyber State of the World." Presentation, 2010 CD&E Conference, Norfolk, VA, December 7, 2010.

Department of Homeland Security. *Progress in Developing the National Asset Database.* Washington D.C.: United States Department of Homeland Security, Office of the Inspector General, 2006.

Detwiler, Bill. "10 Jobs Within Cybercrime Organizations." *TechRepublic*, April 2, 2010.

http://www.techrepublic.com/blog/itdojo/10-jobs-within-cybercrime-organizations/1632 (accessed December 17, 2010)

Government Accountability Office (GAO). *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed*. Washington D.C.: United States Government Accountability Office, 2010.

"Hackers Catch World Cup Fever." *BBC News*, August 23, 2002.

http://news.bbc.co.uk/2/hi/technology/2210186.stm (accessed January 20, 2011).

Hall, Andy and Andy Winter. "WikiLeaks: Hackers Now Set Sights On Paypal." *Sky News Online*, December 9, 2010.

http://news.sky.com/home/uk-news/article/15850393 (accessed January 20, 2011).

"Huge Threat to Power Grid." *WorldNetDaily*, February 10, 2009.

http://www.wnd.com/index.php?fa=PAGE.view&pageId=111629 (accessed December 13, 2010).

Krebs, Brian. "Mapping the Russian Business Network." *The Washington Post's Security Fix Blog*, October 13, 2007.

http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html (accessed January 16, 2011).

Meserve, Jeanne. "Sources: Staged Cyber-attack Reveals Vulnerability in Power Grid." *CNN*, September 26, 2007.

http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US(accessed December 13, 2010).

Mills, Elinor. "USB Devices Spreading Viruses." *CNET*, November 20, 2008.

http://news.cnet.com/8301-1009_3-10104496-83.html (accessed December 10, 2010).

Neild, Barry. "$250K Microsoft Bounty to Catch Worm Creator." *CNN*, February 13, 2009.

http://articles.cnn.com/2009-02-13/tech/virus.downadup_1_conficker-downadup-infected?_s=PM:TECH (accessed January 12, 2011).

Paget, Francois. "Cybercrime Organizations Turn to 'Mafia-Style' Structure." *McAfee Blog Central*, October 19, 2009.

http://blogs.mcafee.com/mcafee-labs/mafia-style-cybercrime-organizations (accessed September 13, 2011).

Prince, Brian. "Critical Infrastructure Security a Mixed Bag, Report Finds." *eWeek.com*, January 28, 2010.

http://www.eweek.com/c/a/Security/Critical-Infrastructure-Security-a-Mixed-Bag-Report-Finds-362438/ (accessed December 17, 2010).

"Prison Urged For Mafiaboy." *Wired*, May 20, 2001.

http://www.wired.com/politics/law/news/2001/06/44673 (accessed January 14, 2011).

Poulsen, Kevin. "Slammer Worm Crashed Ohio Nuke Plant Network." *SecurityFocus*, August 19, 2003.

http://www.securityfocus.com/news/6767 (accessed December 12, 2010).

Poulsen, Kevin and Kim Zetter. "U.S. Intelligence Analyst Arrested in Wikileaks Video Probe." *Wired*, June 6, 2010.

http://www.wired.com/threatlevel/2010/06/leak/ (accessed January 20, 2011).

Roberts, Paul F. "Zotob, PnP Worms Slam 13 DaimlerChrysler Plants." *eWeek.com*, August 18, 2005.

http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/ (accessed December 13, 2010).

Ross, Nick. "Lulzsec teams up with Anonymous." *ABC*, June 20, 2011.

http://www.abc.net.au/technology/articles/2011/06/20/3248520.htm (accessed October 20, 2011).

Session, Willie. "Cyber Crime and US Law Enforcement." Presentation, 2010 CD&E Conference, Norfolk, VA, December 7, 2010.

Singel, Ryan and Kevin Poulsen. "Your Own Personal Internet." *Wired,* June 29, 2006.

http://www.wired.com/threatlevel/2006/06/your_own_person/ (accessed December 3, 2010).

Schwartau, Winn. "Winn Schwartau Predictions and More..." Winn Schwartau. Author. Speaker. Thinker.

http://www.winnschwartau.com/winnpredicts.html (accessedDecember 5, 2010).

Taylor, Jerome. "Who are the Group Behind this Week's CIA Hack?" *The Independent*, June 16, 2011.

http://www.independent.co.uk/news/world/americas/who-are-the-group-behind-this-weeks-cia-hack-2298430.html (accessed October 20, 2011).

Warren, Peter. "Hunt for Russia's Web Criminals." *The Guardian*, November 15, 2007.

http://www.guardian.co.uk/technology/2007/nov/15/news.crime (accessed January 15, 2011).

Zetter, Kim. "DHS: Anonymous Interested in Hacking Nation's Infrastructure." *Wired*, October 17, 2011.

http://www.wired.com/threatlevel/2011/10/hacking-industrial-systems/ (accessed October 17, 2011).

Zetter, Kim. "Did a U.S. Government Lab Help Israel Develop Stuxnet?" *Wired*, January 17, 2011.

http://www.wired.com/threatlevel/2011/01/inl-and-stuxnet/all/1 (accessed January 17, 2011)

Zetter, Kim. "Iran: Computer Malware Sabotaged Uranium Centrifuges." *Wired*. November 29, 2010.

http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges (accessed December 10, 2010).