Sean B. Hoar
"*International Trends in Cyber Law Enforcement: The Dark Side of the Internet*"
International Security National Resilience Conference 2010
Abu Dhabi, United Arab Emirates
March 3, 2010

Good afternoon. It is a privilege to be with you, and an honor to be among the speakers at the ISNR 2010 Conference. My hope it that I will in some way contribute to the high quality of information you have and will continue to receive in this forum.

(PwrPt #)
1. The Internet . . . it has created a whole new world . . . a virtual world that is constantly and rapidly evolving. A world in which our dreams have become realities; where the best and the brightest have created a technological marvel that has surpassed all imaginable expectations; a digital utopia that has brought out the best of humanity . . . but also the worst . . . it has created an anonymous environment where cowards, criminals and terrorists operate on the dark side with impunity . . . It is those cowards, criminals and terrorists that have provided the foundation for my presentation to you today.

2. But first, a few statistics about the technological marvel we call the Internet:

In the time it takes for me to make this presentation . . . over

37,000 blogs will be posted on the Internet; over 1,300,000 "tweets" will be sent on Twitter; over 7,292,000 people will log on to Facebook; over 41,666,000 videos will be watched on YouTube; and over 118,000,000 searches will be conducted on Google. This technological phenomenon has not only changed the way we communicate, it has changed the way we live.

3. At the ISNR 2010 Conference, it is important that we look at international trends in cyber law enforcement. In doing so, it is helpful to understand the backdrop against which these trends have developed - and perhaps it will allow us to better confront the challenges that lay ahead. As you probably all know, the Internet was developed to facilitate the sharing of research, and was designed as a network of nodes such that if one failed, the remaining would exist to allow communication to continue. Security was not part of the original architecture . . . The military and academic personnel who developed the initial Internet nodes never imagined that it would develop into a world-wide network of networks that could be used to steal data, commit fraud, or facilitate terrorist financing! Yet that is precisely what the dark side of the Internet has become . . . As I speak, it is being used to disseminate malware, hack into computer networks, distribute spam, commit financial fraud, steal intellectual property, sell narcotics and exploit children. I will review the various crimes being committed on the Internet today, discuss some who have committed those crimes, how they were brought to justice, and identify the challenges and opportunities that lie before us.

4. The first major trend in cyber crime is the dissemination and use of malicious software, or "malware." As you know, malware is software developed for the purpose, generally, of altering or stealing data, or doing harm to computer networks. Malware is often defined by how it is executed, how it is spread and/or what it is intended to do. Malware generally takes the form of a virus, a worm, a Trojan horse, a backdoor, crimeware, or spyware.

5. The creation and dissemination of malware is continuing to grow at an exponential rate. In the last six months of 2009, malicious web sites grew 225%. Of all the user-generated comments to blogs, chat rooms and message boards, 95% were spam or malicious. Of all the searches for trending news and the new Internet vernacular "buzz" words, 13.7% led to malware. The majority of malware connects to host Web sites registered in the U.S.A. (51.4%), with China second (17.2%), and Spain third (15.7%).

6. The dissemination of malware is very strategic and it quickly finds its way to legitimate sites that you regularly visit. In fact, 77% of web sites with malicious code are legitimate sites that have been compromised.

7. A primary means of malware dissemination is email. Not surprisingly then, in the last six months of 2009, 85.8% of all emails were spam. Spam , as you know, is unsolicited, junk email mail. Most of it attempts to purvey pharmaceuticals, such as sexual performance enhancing substances like viagra, or

narcotics, such as hydrocodone. The remainder of spam attempts to purvey counterfeit products. As it turns out, 81% of emails during the second half of 2009 contained malware or a link to something that contained malware. Since email is such a rich source for the dissemination of malware, it is also not surprising that in the last month or so of 2009, it was reported that tens of thousands of Hotmail, Gmail and Yahoo email accounts were hacked and passwords stolen and posted online. Much of this may have actually been the creation of bulk email accounts - which is a related problem - because criminals can buy bulk email accounts for a fraction of the effort it might take to hack into and steal information from them. A related trend involved an increase use of phishing lures, a form of spam used to commit financial fraud. The use of these phishing lures doubled in the second half of 2009, representing 4% of spam email.

8. Part of the malware trend involved data stealing attacks on computer networks. During the last half of 2009, 58% of data-stealing attacks were done via the Internet, and many of these attacks involved data-stealing code.

9. Over one third of all attempts to infect the Internet with malicious code begin in China, with other attempts constantly being made throughout the world, but at much lesser percentages per country. It is truly international in scope, and shows no signs of slowing down.

10. The development and dissemination of malware is driven

by money - big money. It is a multi-billion dollar tax-free industry!! Consequently, it should be no surprise that it parallels the growth of what is referred to as web 2.0 adoption in the workplace. This is a reference to new generation digital applications, social networking sites and search engines. The smart criminals will always go where the money is, and because more potential victims are using popular social networking sites for personal and commercial purposes, the smart criminals target those sites for malicious purposes. And because a primary use for individuals and businesses are search engines, these sites are primary targets.

11. The top 100 most visited web properties tend to be social networking or search engines. The dark side of the Internet is not just the malicious criminal behavior targeting these top sites, but the millions of web sites on the bottom or tail end of the Internet that are junk and scam sites, specifically set up for fraud and abuse.

12. The "webscape," or the content and appearance of the Internet, is constantly evolving and as we become more technologically sophisticated, so do the criminals - and they usually have the time and money to stay a step or two ahead, making security a constant challenge.

13. As a result of all this, the most prevalent trend in cyber crime is the use of malware in new generation web content - social networking sites and search engines - to exploit weaknesses within the Internet infrastructure and affect the

greatest number of victims. User-created content is currently being creatively leveraged to compromise sites with good reputations and victimize ever more consumers.

14. Major events also provide fodder for attacks designed to steal personal or business information - where there are major events there will be major scams. Whether it is a major sporting event like the Olympics or the World Soccer Cup, health concerns like the H1N1 scare, natural catastrophes like the earthquake in Haiti, or issues related to the economic crisis, hackers will insert malicious code into sites visited by consumers interested in the content. It might be someone purchasing a sporting event ticket, or someone donating money to a charitable cause, and even if the consumer gets a legitimate ticket, or the money actually makes it to the charitable cause, their credit card account information may be stolen, or a key logger or similar application may be downloaded and inserted into their own computer system for future and continual theft.

15. Although the insertion of malware into computer networks is done for different reasons, it is primarily for profit or strategic advantage. If it is done for profit, it is usually done by criminals and criminal organizations, or terrorists to fuel their causes. Identity theft is a multi-billion dollar industry and a low risk source of money for criminal and terrorist groups. If it is done for strategic advantage, it is usually done by governments seeking other government's "state secrets," or by terrorist groups seeking to exploit sensitive data within the critical infrastructure of targeted countries or cities. Other types of

attacks include distributed denial of service attacks, where an automated attack involving thousands or tens of thousands of communications are sent simultaneously to a targeted site with the intent to congest the digital pipes and shut down communication to the site. This sometimes involves extortionate requests where the attacker agrees to stop the attack if certain ransom is paid. Web site defacement is another type of attack which is often politically motivated and targeted upon corporate or government sites.

16. An example of a successful investigation and prosecution of a network intrusion case involved Edwin Pena, a Venezuelan citizen, and Robert Moore, a United States citizen. Pena and Moore hacked into the networks of Voice Over Internet Protocol (VOIP) providers around the world and resold the hacked VOIP services for a huge profit. They were both prosecuted in the United States. Moore was sentenced to serve 24 months in prison, and Pena just pled guilty last month and is awaiting sentencing.

17. An indication of the high value of malware to cyber criminals is that a competitive market place for malware has emerged. It is so competitive that one application, a relatively new Russian Trojan horse called Spy Eye, removes its primary competitor, Zeus, from the victim computer. This gives Spy Eye exclusive access to user names and passwords on the victim computer. Spy Eye and Zeus are examples of Trojan-making toolkits designed to give criminals easy means of creating their own "botnet" networks of password-stealing programs. Spy Eye

sells for about $500 on the black market - the dark side of the Internet - and premium versions of Zeus sell for around $2500.

18. Another example of malware used to commit identity theft are applications called keyloggers. These surreptitious software applications exploit security flaws on victim computers and monitor the path that carries data from the keyboard to other parts of the computer. Monitoring programs are often hidden within e-mail attachments, files shared via peer-to-peer networks, or embedded in web pages – exploiting web browser features. Tens of millions of machines are infected with keyloggers, putting billions in bank account assets at the fingertips of criminals.

19. In December, a New York man named Stephen Watt was sentenced for providing a "sniffer" program to other criminals who used it to monitor and capture data including customer credit and debit card information as it traveled across corporate computer networks. He was involved in one of the largest reported incidents of data theft in the United States and was sentenced to serve 24 months in prison and ordered to pay $171,500,000 in restitution.

20. Data breaches are obviously still a tremendous problem. In the United States, certain laws require certain types of data breaches to be disclosed to the public. When reporting first began in 2005, everyone was shocked to hear that on February 15, 2005, records of 163,000 consumers were accessed by criminals from within the ChoicePoint data base. ChoicePoint

is an information broker, and at the time had one of the more extensive data bases on consumers.

21. Just a few months later, on June 16, 2005, a significant data breach occurred in the data base of a credit card issuer and 40,000,000 consumer records were accessed from the CardSystems data bases.

22. In the United States alone, between January 2005 and February 2010, private records belonging to 345,724,373 consumers were compromised in data breaches.

23. Data breaches are also getting more expensive for the compromised companies. Last year in the United States, it cost companies an average of $204 per compromised customer record and an average of $6.75 million per data breach.

24. As a result of a 2008 data breach, a New Jersey based credit card processing company called Heartland recently agreed to settle law suits by paying VISA $60 million and American Express $3.6 million. Heartland was one of several corporate victims in one of the largest data breaches in the United States.

25. On a more positive note, one of the criminals responsible for the Heartland data breach, Albert Gonzalez, pled guilty in December to hacking into several major credit card data bases. Gonzalez controlled several computer servers which were used to store malicious software and to launch attacks against

corporate victims. In doing so, Gonzalez and his associates used malware to steal tens of millions of credit and debit card numbers, affecting more than 250 financial institutions.

26. As an example of the international flavor of data breaches, in November, hackers from Estonia, Russia, and Moldova were charged with hacking into the RBS WorldPay data base. They compromised the data encryption that was used to protect consumer data on payroll debit cards. Once the encryption on the card processing system was compromised, the hackers raised the account limits on the compromised accounts, and then provided a network of "cashers" with counterfeit payroll debit cards, which were used - in a 12 hour period of time - to withdraw more than $9 million from more than 2,100 ATMs in at least 280 cities worldwide, including in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada.

27. In another example of the international nature of the problem, a Swedish citizen was recently charged with hacking into the Cisco computer system and stole computer code pertaining to the Cisco Internetworking Operating System. He was also charged with hacking into the NASA computer network.

28. A related trend, phishing, is a criminal mechanism which employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

29. Social-engineering schemes use spoofed e-mails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords.

30. Technical subterfuge schemes plant crimeware onto victim computers to steal credentials. They often use systems to intercept online account user names and passwords to corrupt local navigational infrastructures which misdirect consumers to counterfeit websites or route them to authentic websites through phisher-controlled proxies which monitor and intercept keystrokes.

31. In October, the largest number of defendants ever charged in a cyber crime case were indicted in a sophisticated international phishing case where information stolen from thousands of persons was used to defraud financial institutions. 53 persons were charged in the United States and 47 persons were charged in Egypt.

32. As part of the phishing trend, the number of crimeware-spreading sites infecting victim computers with password-stealing crimeware reached an all time high of 31,173 in December of 2008, an 827 percent increase from January of 2008. Although the number of crimeware-spreading sites has decreased slightly since then, it only appears to have occurred because the crimeware is being more selectively directed to sites with the greatest potential of infecting victim computers.

33. Just over six months ago, in August of 2009, unique phishing reports submitted to the Anti-Phishing Working Group - or APWG - reached an all-time high of 40,621. So it remains a tremendous problem on the cyber scape.

34. Consistent with the number of unique phishing reports, in August of 2009, APWG detected 56,362 unique phishing websites, the most ever detected by APWG.

35. Consistent with this trend, 341 business brands were hijacked by phishers in August 2009, the highest number of hijacked brands ever reported, up 10% from the previous record of 310 in March of 2009.

36. Of the brands hijacked, the financial services sector continues to be the most targeted industry sector - which, of course, makes sense . . . the smart criminals go where the money is!

37. While the phishing problem is clearly international in scope, the USA continues to host more phishing sites that any other country.

38. A phishing-related trend involves rogue anti-virus products - called rogueware. Rogue anti-virus products - or rogueware - are applications that lead a computer user to believe their computer is infected with a virus, and cause the user to pay for an application that does nothing, or is the executable file that actually infects the computer. Cyber criminals have found that

these products are some of the most efficient – and increasingly preferred - ways to victimize consumers. Unlike banking Trojans, where cyber criminals have to infect a victim computer and steal data, a rogueware attack simply fools users into paying for worthless software – or forcing them to make a ransom payment. The user is the one willing to pay in order to "disinfect" their computer - or free it from a cyber criminal's control.

39. Cyber criminals profit faster by increasing the proportion of users who pay after downloading rogueware. These techniques have rocketed in the last quarter, with new cyber criminals using ransomware – which doesn't let you use your computer until you buy a 'license.'

40. As I've already referenced, there are different types of malware. Crimeware is one type of malware and it is used to steal personally identifiable information. It is often an application involving data-stealing malicious code designed specifically to be used on customers of financial institutions and co-opts the identity of the financial institution - meaning that it causes consumers to believe they are providing their information to the financial institution. Malware also includes more general data stealing or generic Trojans which are malicious code designed to send information from the infected machine, control the machine, and open backdoors on it to mine data or monitor usage with a keylogger. Other types of malware involve a variety of malicious code which may allow criminals to remotely control a computer for malicious

purposes.

41. The most recent statistics indicated that almost half of all computers connecting to the Internet are infected with some form of malware.

42. And the two countries with perhaps the most users connecting to the Internet, USA and China, are competing for first place as to which one hosts more of what might be perceived as the most dangerous, and perhaps the most profitable, type of malware - a phishing-based keylogger or a Trojan downloader which downloads a keylogger. The moral of this story is that the cyber criminals tend to go where the users are, they tend to want to insert keyloggers, because the more data they can steal, the more money they can make.

43. As of February, 2009, users in the USA, the UK, and China were the primary targets of phishing attacks.

44. During this same time frame, the USA, China, the Russian Federation, France and Germany were the primary targets of crimeware attacks. What this might suggest is that while the broader net of phishing was thrown to capture the most users in the USA, the UK and China, more specific crimeware was targeted at consumers engaged in financial transactions with financial institutions in the USA, China, the Russian Federation, France and Germany.

45. Beyond phishing or crimeware attacks, and often the means

of delivery for those attacks, is the next primary international trend - spam . . . Almost 9 out of every 10 email messages sent across the Internet is spam - or unsolicited commercial email. It s often sent out in bursts of tens of thousands or millions of messages through compromised email accounts.

46. Spam includes a variety of content. Most of the content appears to purvey pharmaceuticals, such as sexual performance enhancing substances like viagra, or narcotics, such as hydrocodone. The remainder of spam attempts to purvey counterfeit products.

47. A Romanian citizen recently pled guilty to harvesting email addresses from colleges and universities in the United States, and then spamming those email addresses in phishing schemes where the recipients would be directed to counterfeit web sites for financial institutions.

48. A number of U.S. citizens along with a resident of Hong Kong were recently convicted in another case. One of the U.S. citizens, Adam Ralsky, known as the King of Spam, was widely recognized as one of the most pervasive spammers in the world. He was eventually caught and sentenced to serve 51 months in prison, and ordered to forfeit $250,000 which was seized from him. One of the schemes perpetrated by Ralsky was what is known as a pump and dump scheme where he would send spam email containing false information for the purpose of inflating or "pumping up" certain stock prices, and would then dump his shares on the market.

49. Financial profit underlies most cyber crime, and one of the trends includes various types of financial fraud. It appears in a variety of forms including identity theft, carding - the selling or trading of stolen credit card account numbers, auction fraud, advance fee fraud, Nigerian 419 scams, high yield investment programs, pyramid schemes, stock fraud, click fraud, and economic espionage.

50. Much of the on-line fraud is so rampant, I expect most of us have experienced it in one form or another. I was somewhat surprised that my own information had been stolen by an employee for one of the financial firms with which I was doing business. On September 6, 2008, I received a letter from my mortgage holder that they discovered that an insider had stolen my information. In doing some further research I learned that on Aug. 2, 2008 the FBI arrested a former employee of my mortgage holder in a scheme to steal and sell personal information. The breach occurred over a two-year period though July of 2008. The insider was a senior financial analyst who downloaded about 20,000 customer profiles each week and sold files with that many names for $500. He typically would e-mail the data in Excel spreadsheets to his buyers. At least some of the names were being sold to people in the mortgage industry to make new sales. So . . . none of us is immune to identity theft if any data repository contains any of our personally identifiable information.

51. Recently I prosecuted a relatively complex identity theft case involving a young man by the name of Jeremiah Mondello.

Given the technology accessible to anyone using the Internet, the case could have happened anywhere in the world. As it turned out, Mr. Mondello was a local high school graduate and a computer genius. Between December 2005 and October 2007 he initiated thousands of separate online auctions using more than 40 fictitious usernames and online payment accounts to sell copies of counterfeit software. He generated more than $400,000 in personal profit.

52. Mondello acquired the victims' names, bank account numbers and passwords by using a keystroke logger. The keystroke logger installed itself on victims' computers and recorded the victims' names and bank account information as the information was being typed. The program then electronically sent the information to Mondello which he then used to establish fictitious usernames and online payment accounts.

53. Mondello pled guilty to criminal copyright infringement, aggravated identity theft and mail fraud and consented to the forfeiture of more than $225,000 in cash proceeds. He also forfeited computer-related equipment used to commit the crime. He was sentenced to serve 48 months in prison. When he is released from prison he will serve three years of supervised release and will perform 450 hours of community service. While he has been in prison, in order to reduce his sentence, he made an anti-piracy video for the Recording Industry Association of America. We thought such a video might be a creative way to get the word out to other young people who

might consider committing on-line crime, including intellectual property theft.

54. Another type of financial fraud is what is referred to as the Nigerian scam, because for many years it emanated from Nigeria. The traditional scam is referred to as the 419 scam as that is the section number of the Nigerian criminal code regarding obtaining property by false pretenses. It usually involves a letter or email message sent to a potential victim stating that they have been identified as a trusted person, although the identical message is actually sent to many recipients. The message attempts to persuade the victim to provide their bank account information in order to receive a few million dollars, or a few billion dollars. The money purportedly has been inherited from a wealthy deceased relative, but is prohibited from being taken out of the country by a corrupt government. Every year, millions of dollars are lost to this type of scam. The scam has many varieties, including an overpayment scam, a check cashing scam, a re-shipping scam, a tax refund scam, a lottery scam, an Internet romance scam, an inheritance scam, an insurance scam, a business opportunities scam, and investment scams.

55. As proof that these scams are alive and well, just a few weeks ago, a Nigerian citizen was convicted of wire fraud for running an advance fee scam on the Internet. The scam enticed people to send money with the false promise that they would receive a greater sum in the future.

56. A few months ago I sold a few things on-line, and much to my surprise one of the first responses I got to my add was someone who attempted to involve me in an overpayment scam.

57. Almost immediately after I had posted an add to sell a couch, I received a message from "Sarah Henshaw" indicating that she was interested in purchasing the couch.

58. I have to admit that I was pretty excited to receive such a quick inquiry.

59. But then she sent a message telling me that she was going to send me a check, that it would cover the expenses of her shipping company, and that she didn't have time to even look at the "item" because of her "work frame." I have to admit being disappointed that my "buyer" was not real, and that it was simply an attempt to over pay me with what would have been a counterfeit check. I would have then been requested to remit back to Ms. "Henshaw" the difference between the item and shipping price and the amount of the check - the overpayment. Had I done so, I would have ultimately been charged by the bank for the total amount of the counterfeit check after remitting to Ms. "Henshaw" the overpayment . . .

60. Another type of financial fraud involves economic espionage. As an example, just a few weeks ago an aerospace engineer was sentenced to serve 15 years in prison after being convicted of acting as an agent of another country while employed by Rockwell and Boeing, from whom he stole

restricted technology and trade secrets, including information related to the Space Shuttle program.

61. Another international trend in cyber crime involves intellectual property theft - IP theft. It is widely recognized as a huge international problem. It is estimated that 90% of the software, DVDs, and CDs sold in some countries are counterfeit, and that the total global trade in counterfeit goods is more than $600 billion a year. In the USA alone, IP theft costs businesses an estimated $250 billion annually, and 750,000 jobs.

62. The USA recently established an Office of the Intellectual Property Enforcement Coordinator (IPEC), a Presidential Cabinet level IP theft enforcement and policy coordinator. It also established an Intellectual Property (IP) law enforcement task force which will work closely with the IPEC.

63. A Saudi citizen was recently found guilty of trafficking in counterfeit Cisco goods. He was convicted of purchasing counterfeit Cisco Gigabit Interface Converters from an online vendor to satisfy a contract he had with the U.S. Marine Corps.

64. A Chinese national was recently sentenced to 30 months in prison and ordered to pay $790,683.85 in restitution for causing hundreds of thousands of dollars worth of counterfeit Cisco computer hardware in China to be exported to buyers in the United States.

65. Two U.S. citizens were recently charged with importing

counterfeit Cisco hardware from China.

66. Another trend in cyber crime is the unlawful sale and distribution of narcotics & other controlled substances via the Internet. The unlawful sale and distribution of confidential government information is also a problem. Illegal exports in violation of trade embargos also occur via the Internet.

67-68. Finally, child exploitation on the Internet continues to be a problem. Millions of images containing child pornography are distributed daily throughout the Internet. Pornography is a multi-billion dollar business and, unfortunately, child pornography drives part of those profits.

69. So what are the challenges facing on-line law enforcement? One of the primary challenges is that it is a technically complex subject matter, and there is a tremendous lack of technically trained investigators, prosecutors, judges and jurors. Also, a highly technical forensic process may be required to acquire and preserve evidence. The process may be time sensitive, the evidence may be fleeting, and special legal process may be required to acquire and preserve evidence. All of this can be overcome, but they are obstacles that can preclude certain on-line enforcement.

70. There are also limited resources to deal with the nature of cyber crime cases. They are data intensive, they compete with other priorities, and they are transnational. Given the transnational nature of cyber crime cases, separate sovereigns

are usually involved, and often there are a lack of treaties or dual criminality provisions. If there are dual criminality provisions, there is then the slow, cumbersome MLAT process. And if all that goes well, there are still the language barriers . . .

71. So how can we overcome the impediments to on-line law enforcement? We need to increase human and monetary resources allocated to fighting cyber crime. This needs to involve increased technical training for investigators and prosecutors. Investigators also need adequate technology to deal with the evolving technology, and increased language training would benefit investigators when dealing with foreign populations. Increased international cooperation is imperative, with fundamental dual criminality standards between all countries. And in order to make sure investigations reach their fullest potential, we need to expand informal networks in all countries so they can be activated for immediate assistance.

72. The increased international cooperation needs to involve a number of things, including uniform financial standards for certain types of transactions and sites. It should also include uniform financial standards for suspicious monetary transaction alerts, and uniform agreements to share seized assets, which constitute proceeds of fraud, with assisting agencies/governments.

73. Finally, at a time when cyber criminals are ever more sophisticated, we need to expand our creativity, and initiate programs to secure vulnerabilities in digital devices connected

to the Internet. One initiative in the USA is called the CyberSafe Initiative - or CyberSafe. CyberSafe is a public service project designed to educate end users of the Internet about the critical need for personal computer security. It is intended to empower them to increase their online security and reduce vulnerabilities in the Internet at the user level, thereby reducing the dissemination of malicious code and the resulting consumer fraud, data theft, and system disruption. Extraordinary challenges require extraordinary action . . . Now is the time for all of us to take ownership of our own corners of the Internet, and take whatever action is necessary to secure it for the future.

Thank you.