Peter Altabef Keynote

7th Worldwide Security Conference
EastWest Institute & World Customs Organization
February 18, 2010 – Brussels

Word Count (actual speech text): ~2,775 / ~26 minutes

[Introduction by Maria Livanos Cattaui, EastWest Institute board]

- Thank you Maria, and let me also thank the EastWest Institute and the World Customs Organization for hosting this important event. It is a privilege to be here, and I appreciate the opportunity to speak with all of you today.
  - This morning, my goal is to present some perspectives on cybersecurity – or the protection of digitized information that is stored and transmitted over networks.
  - In one speech, it is impossible to fully cover this complex topic, but my goal is to provide some foundational elements for consideration in the plenary session and workshops that follow.

KEY POINT: Cyber threats emerged in tandem with cyber benefits

- Let's begin with the story of the Morris worm. The name might sound like a children's bedtime story, but it actually refers to harmful software that nearly crashed the entire Internet.
  - Once introduced to the network, the Morris worm spread undetected from computer to computer, and quickly infected 10 percent of all computers on the Internet.
  - The worm unleashed a data overload that rendered the world's most powerful computers useless and disrupted the Internet for several days.
  - The resulting panic was so bad that many organizations -- including the U.S. Department of Defense – pulled the plug on their Internet connections to protect their systems.

- Very few people today know about the Morris worm, because it struck in 1988 – a time when relatively few people had even heard of the Internet.
  - The Morris worm's historical significance is not that it was the first harmful code to go online. It was not.
  - The real significance is that the Morris Worm sparked the first coordinated effort to fight cyber attacks and to promote cybersecurity.
  - Specifically, the U.S. government funded the world's first Computer Emergency Response Team – or CERT – to protect national security and critical infrastructure.
  - Over time, this concept has expanded and become collaborative, with CERT organizations now operating in more than 40 nations.
  - For the past two decades, some of the most brilliant minds in technology have fought each other to protect – or to attack -- cyberspace.

- Despite the rapid growth in cyber security, cyber criminals have become a permanent part of the Internet's ecosystem. As a class, these people are responsible for billions in financial losses and putting critical infrastructures at risk.

- Interestingly, the battle in the cyber sphere was first predicted more than 170 years ago.
  - In 1838, the inventor of the telegraph, Samuel Morse – no relation to the Morris worm! – described the advent of electronic communications this way. He said, quote:
    - "This mode of instantaneous communication must inevitably become an instrument of immense power, to be wielded for good or evil."
    - His invention was a tremendous milestone, because it was the telegraph – <u>not</u> the Internet – that first liberated information from the confines of location and time.
    - By the 1850s, newspaper stories predicted the telegraph would forever alter government and banking, make newspapers obsolete, and erase hostile national rivalries.
  - A century and a half later, people were making similar predictions, this time about the Internet.
  - The real leap forward with the Internet was liberating information from the constraints of volume and cost.
    - Whereas people paid a high price per word for a telegram, the Internet offers virtually the entire compendium of human knowledge and multimedia creativity, often for a flat monthly rate.

- In many ways, the Internet <u>is</u> fulfilling long-held hopes of humankind -- the "good" that Samuel Morse predicted.
  - Distance learning, telemedicine, e-commerce, virtual communities, and instant global communications are now established realities.
  - The Internet also can dramatically improve productivity. As a result, information and communications technology is now embedded at the core of operations for governments, financial systems, industries and critical infrastructure.

- Parallel with these benefits, we have seen the emergence of the "evil" that Morse warned the world about.
  - The malicious and criminal use of cyberspace today is stunning in its scope and innovation.

- For example:
  - Trojan Horses are software programs that appear to be something you want, but which actually put your computer at great risk.
  - You can infect your computer simply by clicking on a camouflaged e-mail attachment or visiting infected websites.
    - Initially, this illicit software primarily was intended for cyber vandalism – including destruction of data on your hard drive.

    - Now, they are usually designed to avoid detection, and motives range from illicit financial gain to potential attacks by one nation against another.
  - In many cases, these malicious software codes can allow criminals to remotely control an innocent user's computer.
  - The computer continues to function for its owner, but the device has become a "zombie" – a slave to the hacker.
    - Criminals, and increasingly organized gangs, put together armies of zombies with hundreds and even thousands of computers to create a "botnet."
    - Recent research reports indicate that more than 100 million computers are infected with malware that can turn them into pawns for botnet[1] attacks.

- With an army of computers at their command, criminal hackers can tell their zombies to simultaneously bombard anything connected to the Internet, from a website, to a nation's electricity grid.
  - Known as a Distributed Denial of Service attack, the flood of data coming from the zombie army blocks out legitimate traffic and can knock institutions offline and force infrastructure out of service.
  - Criminals actually rent out their botnets to send spam or conduct digital extortion, essentially telling a business to "pay up or we will shut you down."
    - Some gangs will take a credit card payment[2] to launch a denial of service attack.

- Botnets are bad, but they are far from the only challenge for cybersecurity.
  - Viruses, worms, phishing and other techniques are appearing in greater numbers, and they are constantly evolving in complexity.
    - The pace of criminal innovation requires constant effort to keep countermeasures up to date.

- Last September, the Center for Strategic and International Studies – or CSIS -- surveyed executives in 14 countries across the Americas, Europe, Asia and the Pacific.
  - 54 percent of executives said they had experienced a large-scale denial of service attack.
  - 70 percent said they had dealt with other problems, including network vandalism, insider data theft or loss of sensitive data.

- Industrial control systems are an important category of systems that can be vulnerable. These systems control equipment used in manufacturing, utilities, oil refining and other settings.
  - In general, these systems were not designed for network connections, but many[3] are now linked to the Internet for management convenience and productivity.
  - Malicious commands sent over the Internet can disrupt operations and even cause physical damage to equipment.[4]

- In addition, cybersecurity researchers generally agree that state actors and hackers acting from national pride could engage in cyber attacks and espionage against other nations.[5]

KEY POINT: Current cybersecurity solutions are essential and significant, and broader efforts are also necessary

- I have only been able to scratch the surface about the challenges to cybersecurity, but we need to turn our attention now to solutions.

- Three basic elements required for security are governance, technology and education.

- Governance refers not to an actual government, but to the systems and policies that govern the use of technology in homes, offices and networks that serve corporations and governments.
  - Governance ranges from regularly changing passwords on a personal account to intensely complex and multilayered security defenses across large organizations.
  - Small and medium businesses, however, often do not have the resources to deploy or manage large-scale security, and a typical consumer solution is insufficient to address the more complex needs of a business.

- On the technology front, many small and medium enterprises increasingly use managed security solutions. Expert "hosting" providers, including Dell, can manage security services for a business, often on a subscription basis.
  - Another element of technology is the need to upgrade existing systems, including industrial control systems that are particularly vulnerable to attack.
  - Moving forward, security must be designed into new software and hardware products from the earliest planning stages.

- Education is also a multi-faceted element. Individuals must have opportunities to educate themselves about cybersecurity risks and how to deal with them.
  - Education also means expanding the ranks of well-trained technology professionals that specialize in cybersecurity.

- These basic steps are essential, and even broader efforts will be necessary to ensure security as Internet access continues to expand worldwide.

KEY POINT: Cyber crime undermines the trust needed for effective economies and societies in developing as well as first-world nations.

- As ubiquitous as the Internet might seem to us, only a quarter of the world's 6.8 billion people are on the net today.[6] The limiter is access, not interest.

- The most likely tool for many of the remaining 5 billion world citizens to become cyber users is the ongoing spread of mobile communications.

- For emerging nations, digital information and communications represent some of the biggest levers for expanding economic growth -- and mobile communications is playing a key role.
  - The introduction of fourth-generation wireless service, now emerging, holds tremendous potential to bridge the world's digital divide.

- As access to online communications expands, strengthening and ensuring cybersecurity becomes increasingly important.

- A significant consideration that is often overlooked is the risk that the increasing rates and scale of cyber attacks threaten to undermine essential trust -- trust among nations, commercial and non-commercial institutions, and individuals … trust that is necessary for economies and societies to promote the common good.

- The philosopher and economist Francis Fukuyama, in his book "Trust: The Social Virtues and the Creation of Prosperity," asserts that economic activity is more than GDP. Instead, he says economics is best understood as a form of human sociability.[7]
  - Economies at local and global levels rely on associations of people who engage in production and exchange. Success requires widely distributed trust in order to generate widely distributed benefits.
  - In other words, trust is an essential enabler for strong communities that can support vibrant economies.
  - Without trust, communities are diminished, and economies slow and even decline as productivity moves in reverse.

- What is at risk in the cyber fight … is trust in the very technology that offers the best hope for sustained economic development and individual opportunity.

KEY POINT: Interconnectedness mandates multilateral coordination

- To ensure this trust, we must supplement governance, education and technology. Broad public-private collaboration is necessary, as was shown in a landmark security test.

- In 2007, the consulting firm Booz Allen Hamilton conducted a mock cyber attack in the U.S. The exercise involved senior leaders from industry, government, and academia who were assigned to mount or defend against a massive cyber attack.[8]
  - Specific details were not released, but participants did say afterwards that the exercise revealed the need for greater preparedness to protect government operations, critical infrastructure and banking.

  - One of the key lessons was that, because of our vast interconnectedness and interdependence, cybersecurity is too large and complex for any single entity to handle alone.

- The Internet's technology structure actually points the way toward a solution.
  - The Internet is not a monolith. Instead, it is a confederation of private and public networks that have agreed to use the same technology standards -- and at a basic level, to fundamentally trust each other's information and the software behind it.
  - This collaborative approach can be extended to cybersecurity by achieving a multilateral consensus on basic technology standards for cybersecurity, definitions of crimes, and the will to enforce the law and prosecute violations … in other words, to demonstrate the "full faith and backing" of each jurisdiction for the fundamental integrity of cyberspace.

- There are efforts to move in this direction, including multilateral cybersecurity initiatives within the UN, the OECD, the European Union and other entities.[9]
  - The challenges include finding an effective balance between security and civil liberties as well as the specific and sometimes conflicting interests of different governments and constituents.
  - Despite sincere efforts, a cohesive and coordinated approach that reflects existing political structures has remained elusive at the regional – much less global – levels.
  - However, this does not mean that a cooperative multilateral approach to cybersecurity is impossible.

- In fact, we have historic and contemporary models of international collaboration, even if the examples are not directly related to technology.
  - The Treaties of Westphalia in the mid-1600s ended a century of religious wars in Europe.[10]
  - In modern times, nations with diverse and competing interests have established the Law of the Seas and the Outer Space Treaty.
  - The International Telecommunications Union, the United Nations Children's Fund, the World Health Organization and the General Agreement on Tariffs and Trade all emerged from the United Nations.

- These efforts may not be perfect, but they have advanced the common good.
  - We should not be naïve, because nations cannot simply reach a multilateral consensus and then expect lasting change and long-term cybersecurity.
  - We can, however, move towards deeper and broader collaboration that supports a rapid response to the continuous evolution of cyber risks.

- The need for a multilateral effort is why Dell is at this conference, and it is why we are a founding sponsor of the EastWest Institute's' Cybersecurity Initiative.
  - The institute launched the Initiative in 2009 to:

  - Build trust among nations on IT issues,
  - To improve security for information systems,
  - To reduce damages from cyber crimes and attacks,
  - And to enhance nation-state security through better cooperation and infrastructure protection.

- The Cybersecurity Initiative is neither the first nor the only international effort to seek solutions.
  - However, EWI's approach to intractable global challenges holds special promise.
    - The institute has a well-established process to convene diverse parties, reframe security challenges, and mobilize resources to implement solutions.
    - The EWI is already working with Russia, China, the US, India[11] and others to:
      - Create new and effective international collaborative mechanisms and trust,
      - To reframe issues and develop consensus proposals for new agreements and policies,
      - And to champion and mobilize the resources needed to implement high-impact proposals.

[Pause]

- Since the introduction of the telegraph's early potential, the world has come too far with electronic communications to now lose this opportunity to direct the cyber sphere to positive and productive use.
  - The Cybersecurity Initiative is a worthy effort from an organization with a history of making a positive difference.

[PAUSE]

- Before I close, I would like to move this topic from the abstract and look at one example that illustrates the importance of cybersecurity for the real world.

- Dell's YouthConnect program provides philanthropic support for technology-access programs in India, Brazil, Mexico, China, Morocco, South Africa and other locations where disadvantaged youth had no previous access to technology.

- One beneficiary is the American India Foundation's Digital Equalizer initiative, which provides computers and teacher training to under-resourced schools in India.
  - The foundation has shared the story of a boy named Hemant, from a high school in the village of Meghpar Titodi.[12]
  - His original ambition was simple: to find any job to help feed, clothe, and house his family. At heart, though, Hemant is an artist, even if he was limited to doodling on the back pages of his tattered school notebooks.
  - When the Digital Equalizer program came to his school, Hemant touched a computer for the very first time.

- He began using the Microsoft Paint program, and the experience not only helped develop his artistic talent, it also affirmed his faith in himself and his future.
- At last report, the school did not yet have Internet connectivity, but Hemant was looking forward to the day when he could use the Internet to open up new worlds of information and opportunity.
- He could be an animator for Pixar some day, and we could all appreciate his work!
- Young Hemant and billions of people like him might not know it, but they are counting on us to preserve and protect the cyber sphere, which can be such an important key to achieving their dreams.

- Hemant's story is not unique. Many non-profit organizations are achieving tremendous results using information technology in the fight against poverty.
  - Success, however, is predicated on a high degree of trust.
  - Any massive loss of trust resulting from cybercrimes could derail economic growth and set back the improvement in living standards worldwide.
  - Our assessment of cyber risk, therefore, must include the social and economic opportunity costs of individuals and enterprises that are—or become--unwilling to use advanced communications technology ... because they are concerned about the risks of cybercrime.

- I hope you will join me in supporting the East West Institute's Cybersecurity Initiative and its partners as we jointly work to ensure a trustworthy cyber sphere that serves the legitimate needs of governments, institutions, businesses and individuals worldwide.

# # #