

Media Contact:

Amy Carthew
Public Relations
P] 202.654.0929, F] 202.393.7797; E] acarthew@spymuseum.org

The International Spy Museum Unveils *Weapons of Mass Disruption*, A New Frontier in Espionage and Terrorism

Museum launches new gallery addressing cyber security threats and special programming around October's National Cyber Security Awareness Month; addresses what President Obama calls a "weapon of mass disruption"

Washington, DC (September 8, 2009)– On October 2, 2009, the International Spy Museum (SPY) will unveil *Weapons of Mass Disruption*, a new gallery showing how a team of cyber spies, terrorists, or criminals, armed with weapons no more sophisticated than common laptops, can turn power lines into battle lines.

The exhibit serves as a wake-up call about the importance of improving cyber security, which President Obama signaled he would make a priority for his administration. “It’s now clear, this cyber threat is one of the most serious economic and national security challenges we face as a nation,” President Obama cautioned as he outlined his cyber strategy earlier this year. He continued, “It’s also clear that we’re not as prepared as we should be.”

In an exclusive interview with SPY, Director of National Intelligence Dennis Blair compared the lack of safe guards on the Internet to the “wild west of 1870.” Emphasizing the administration’s commitment to protecting America from a cyber attack, he said “We would like to be more effective so that [cyber security] doesn’t become a crisis priority issue.”

Mike McConnell, former Director of National Intelligence, also in an interview with SPY, stressed that “We have a new administration. We have new priorities. The President has obviously articulated in a way that hasn’t been articulated before his concerns regarding cyber threat.”

Remarking on the emergence of this threat co-chair of The 9/11 Commission Report, Lee Hamilton said that “Building a nuclear bomb takes a lot of sophistication, a lot of know-how. A cyber attack can be done from a computer, located anywhere in the world, by a single person.”

The opening of *Weapons of Mass Disruption*, which coincides with the beginning of the Department of Homeland Security’s Cyber Security Awareness Month, depicts attacks that have taken place across the globe including in Australia, Korea, and Estonia, providing a glimpse into the vulnerabilities of international networks.

Underscoring this vulnerability, in an interview with SPY, Richard A. Clarke, former Special Advisor to the President on Cyber Security, noted that “The United States has seen somebody get into its electric power grid and put logic bombs that could bring down the power grid. This is the equivalent of someone in real space laying TNT around power grid facilities throughout the United States except they have done it in cyber space.”

Weapons of Mass Disruption is based on eye-opening research and exclusive video interviews including Director of National Intelligence **Dennis Blair**; Special Advisor to the President on Cyber Security **Richard A. Clarke**; co-author of The 9/11 Commission Report **Lee Hamilton**; Vice Chairman of the Senate Select Committee on Intelligence **Senator Christopher “Kit” Bond**; and former CIA Director **R. James Woolsey**.

Through the use of multi-media, *Weapons of Mass Disruption* imagines the potential devastating impact of a coordinated attack. A successful cyber strike on America's power grid could include blackouts, the breakdown of water and sewage treatment capabilities, the crippling of transport and communications systems (including those of the military), the uncontrollable spread of epidemic diseases, the near-total cessation of economic activity, and widespread civil unrest bordering on chaos.

“Cyber terrorism is a new and dangerous frontier in twenty-first century espionage,” said Museum founder and Chairman Milton Maltz, who has served in the NSA. “Cyber warriors who respect no boundaries require neither passports nor visas to enter our country. From thousands of miles away they can penetrate our defenses, initiate devastating attacks and produce havoc and disorder on an epic scale – all with the use of a home computer,” he said.

Peter Earnest, SPY's founding Executive Director and former CIA operations officer, added, “Few such clandestine threats now pose a greater risk than the possibility that America's digital infrastructure could be attacked, hijacked and even destroyed by cyber intruders working singly, in groups or as part of large, officially sanctioned efforts within nation states.”

The gallery asks viewers to consider, “What would happen if cyber spies break America's security codes – could power lines turn into battle lines?” Answering this question, the gallery describes a series of network attacks on Department of Defense computers during the military's preparation for action against Iraq and notes that such cyber attacks are not rare.

According to a study by US Computer Readiness Emergency Team (US-CERT), in 2008, cyber attacks on U.S. government networks climbed 40 percent. US-CERT is the operational arm of the national cyber security division at the Department of Homeland Security.

Exemplifying this trend, on July 4, 2009, a powerful, coordinated cyber attack successfully disrupted public access to U.S. and South Korean websites. Targets included the National Security Agency, State Department, New York Stock Exchange, and *The Washington Post*.

Coupled with *Weapons of Mass Disruption*, SPY will provide educational programming throughout October ranging from a panel of distinguished experts exploring emerging cyber threats, to an in-depth look into Chinese cyber trends with a retired Senior US Army Counterintelligence Special Agent.

“The gallery opens on the heels of the eighth anniversary of the events of the Sept. 11 attacks,” noted Maltz. “Those attacks exposed our vulnerability to those intent on causing death and destruction inside the United States. They also brought into bold relief the unsettling prospect that future attacks from unknown sources are both possible and probable. If we take only one lesson from that terrible day, it should be that our security as a nation depends on our ability to

imagine the unimaginable – to foresee as best we can not just overt threats, but those that may be growing covertly, behind a veil of darkness, distance and deception.”

“Our response, you can say for sure, is inadequate,” added Hamilton, “We are just not prepared for it.”

###

The International Spy Museum is located at 800 F Street, NW in Washington, DC's historic Penn Quarter, within four blocks of the National Mall, directly across the street from the National Portrait Gallery, and within one block of FBI headquarters and Ford's Theatre. The Museum is conveniently located near the Gallery Place/Chinatown Metrorail station serviced by the red, yellow and green lines.