Winn Schwartau Predictions and More...

"Electronic Pearl Harbor"

Winn Schwartau testified before Congress on June 27, 1991

(Coined the phrase)

"Electronic Pearl Harbor"

CIA Director John Deutch testified before Congress, June 26, 1996

On June 27, 1991 I was asked to report to the Congressional Subcommittee on Technology and Competitiveness, Committee on Science, Space and Technology about the state of security in the private sector and government. The following quotes (available from the committee as well) sum it all up.

"Government and commercial computer systems are so poorly protected today they can essentially be considered defenseless - 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."

At the time detractors said I was *"overstating the condition*" and *"cyber-terrorism simply doesn't exist."* They were wrong then and many are still wrong about my other predictions. My predictions since the late 1980's have been right on.

For that I am sorry. I wish someone had listened. Here is a sampling.

- 1984-1990: Enigma and Compsec II (basis for the Novel DoD C2 network security system) employs Program Whitelisting as a malware deterrent. No one seemed to care.
- 1989: Data viruses and macro viruses will come our way and not need executable code to spread or infect. 1996: Word Macro virus is the biggest fastest spreading virus in history.
- 1989: Coined the word HERF Gun and EMPT Bomb. 1996: Both now in popular lexicon.
- 1990: The government will need to implement its own crypto system to control their hegemony over security and information. 1993: The Clipper Chip.
- 1990: Warned Congress and America about dangers of Cyberterrorism: was labeled “Chicken Little”.
- 1990: Sold C2 Network Security system (created in 1985) to Novel and Centel Federal.
- 1991: Coined the term, Electronic Pearl Harbor in U.S. Congressional testimony and submitted papers.

- 1991: Chipping, the intentional modification of integrated circuits to do malicious things will come soon.
- 1992: US News and World Report and Nightline report on chip-based computer virus to defeat Iraqis. I proved it was a hoax within 1/2 hour. 1994: First commercial chipping example with modified keyboards that spewed out dirty words when not used.
- 1993: Coined term "Information Warfare". Didn't know it was classified at the time. 1994-1996: Information Warfare goes mainstream.
- 1993: Founded InfowarCon, world's first and still largest conference on Cyberterrorism
- 1994: HERF Guns, the nuclear weapons of the nuclear age are the coming 'thing.' 1995: Government holds secret DEW (Directed Energy Weapons conference at Mitre Corporation.
- 1994: (November) Predicted Cyber-Civil Disobedience using Denial of Service attacks on the Internet. 1995 (November): First attacks of this style occur in France. December Italy. February 1996, USA. March, Mexico.
- 1995: Call the "*Most Dangerous Man in America, and the Most Valuable*" by former CIA Case Officer.
- 1995: Denial of Service attacks are the only useful attacks any more. 1995-6: Denial of Service 'events' are occurring all over. Heightened sensitivity to DOS.
- Named the "*Civilian Architect of Information Warfare*" by U.K. Admiral Patrick Tyrrell
- 1995: Predicted that Time is the metric by which security can be measured. Established first formulas for measuring security.
- 1996 "Electronic Pearl Harbor" made mainstream by CIA Director John Deutsch
- 1996: Exported US commercial products will contain intelligence and military Trojans. Proactive Defensive Information Warfare.
- 1996: Designed Internet-wide system to protect against DOS.
- 1996: Predicted malicious code will be found to be cause of many DOS events.
- 1996: In New York *Newsday* editorial, declares use of Microsoft products and OSs a National Security threat.
- 1996: HERF weapons will come out of the closet within 12-18 months, whether the military likes it or not. Several DOS attacks will be found to use this technology.
- 1997 Schwartau's "Infowar.Com" web site breaks 2Million hits per month
- 1998: Vice President Al Gore adapts Schwartau's *Electronic Bill of Rights* as his own.
- 1998: Congress holds hearings on HERF/EMP and financial sector weaknesses to such attacks.

- 1999: Introduced *Time Based Security* as a method to measure and quantify network and information security.
- 1999-2002: More HERF and EMP hearings in Congress. They finally care.
- 1999: Predict Deception will become key network defense technology.
- 2000: Security is all about people. Not technology. People buy in to this quickly.
- 2001: Schwartau's Ethics book called the "*Best Book Ever Written on Security,"* Dr. Fred Cohen, Sandia National Labs.
- 2002: New Security Triad will replace the old cyber-only model.
- 2002: Named one of the *Most Influential Thinkers in America*, Network World.
- 2002: Named Adjunct Professor, Norwich University
- 2002: Developed mathematical model to measure the security of people and administrators in an Enterprise.
- 2003: 10th Anniversary of InfowarCon. (15 shows) Partnership with world's largest conference firm: Reed/Elsevier.
- 2003: St. Petersburg College Partnership.
- 2005: Terrorists are using Internet. Winn predicted 1990 in front of Congress.
- 2005: During DHS National Conference Keynote Speech, 25% of audiencwalks out during "Why We Must Kill Political Correctness for Security portion". DHS management was thrilled.
- 2006: Many American Citizens support organized crime and terrorism through ignorance.
- 2007: China attacks US Infrastructures as part of Class III IW. Winn predicted: 1992.
- 2007: Voted one of the *Top 5 Security Thinkers for 2007* by *SC Magazine.*
- 2007: Co-Founded SCIPP International as the Security Awareness Certification organization for Enterprise users.
- 2007: Named one of the T*op 25 Most Influential People for 2008* by *Security Magazine.*
- 2008: "Beyond Information Warfare" – new book – says we are all wrong.
- 2008: US Government finally considering EMP as offense and effects of attacks on US infrastructure.
- 2008: Sold InfowarCon to Association of Old Crows
- 2008: Data Breaches affect all 300M Americans. Class I Information Warfare in full global swing.
- 2009: EMP, HERF are finally recognized as threats to CIP… 20 years later.
- November 2009, was named one of the *Top-20 security industry pioneers.*
- 2012: World-Cyber-War I has begun. Damn. I wish I had been wrong.

- 2009: Government finally acknowledges ‘Chipping’ is a threat to U.S. national security and military preparedness.
- 2009: Nation-state and NGO cyberwar is now part of every force projection doctrine.
- 2009 Named Chairman, M.A.D. Partners, LLC
- 2009: Smart phones will be the next attack vector for all bad hackers.
- 2010: First mobile bots and hostile code demonstrated
- 2011: Mobile infections in app stores begin life cycle growth (a la virii, 1988+)
- 2011: Between LulzSec and Anonympous, cybercivil disobedience and hactivism move to the forefront of internet activities.
- 2011: DHS says embedded hostile software and hardware is entering the U.S.
- 2012: China admits massive hacking and ‘p0wning’ of US infrastructures.
- 2012: StuxNet (et al) first well publicized US cyber weapons
- 2012: DEW hits the field.

Thanks for asking. We're still thinking.

Winn Schwartau