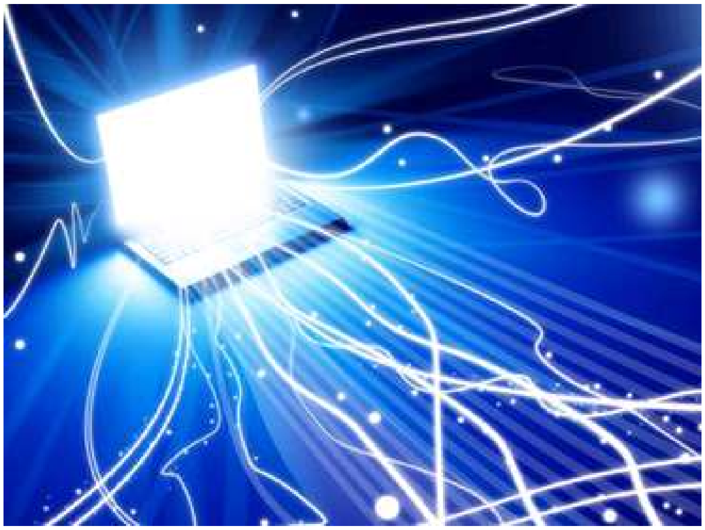
RT QUESTION MORE.

Is cyberwar hype fuelling a cybersecurity-industrial complex?

Published: 17 February, 2012, 02:16
Edited: 17 February, 2012, 02:16



Will the next Pearl Harbor really be a cyberattack? Or the cyberwar doomsday scenarios intentionally hyped up by a coalition of major arms manufacturers, the Pentagon, and Internet security firms greedy for profit?

From the President of the United States, to top U.S. military and intelligence officials, to the pundits and anchors on mainstream news network screens – the message is the same: cyberwar is coming.

As described, the threat is terrifying: an invisible enemy that can destroy our lives and livelihood with a few strokes on a keyboard. Armies of cyberwarriors who can bring down power plants, derail trains, force airplanes to fall out of the sky and wreak massive havoc on the United States.

Just last month, FBI Director Robert Mueller warned congress that threats from cyber-espionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States. Last June,

U.S. Defense Secretary Leon Panetta warned a Senate panel that “*the next Pearl Harbor we confront could very well be a cyber attack that cripples our grid, our security systems*.”

Upon assuming office in 2009, President Barack Obama declared cyberspace a strategic national asset.

“Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer,” Obama said. “*A weapon of mass disruption*.”

But is “*cyberwar*” really a threat? Is the U.S. truly in danger of a catastrophic cyber attack on the scale of a Pearl Harbor? According to a growing number of security experts, the answer is no.

“*There is no chance whatsoever that nuclear power plants will be hacked, that electric infrastructure would be hacked and taken down for any significant period of time,” said Jim Harper, Director of Information Policy Studies at the CATO*

Institute in Washington. “The worst we can expect is disruption – that's not war, it doesn't really terrorize. So the threats are serious but they're not to the level of war on terror."

And yet many top officials who once helped develop the war on terror strategy are now leading experts in the area of cyberwar.

Former U.S. Homeland Security Secretary Michael Chertoff has been urging Congress to pass legislation to protect hospitals, power plants and other sites from cyber attacks. Chertoff, who co-founded the Chertoff Group, a security-consulting firm, warns that a cyberattack could be “as consequential in terms of the economy, maybe even in terms of loss of life, as things we typically associate with war fighting.”

Mike McConnell once headed the National Security Agency. Now a vice-chairman at Booz Allen Hamilton and leading the firm's cyber work, McConnell is on a campaign to raise awareness of the threat of such attacks being used against the US. *"We’re the most vulnerable nation on earth to a cyberattack.”*

Booz Allen frequently works with the Defense Department and has recently launched a "Cyber Solutions Network" service, which advices businesses and governments on how to defend against cyber attacks.

Richard Clarke served as a counterterrorism adviser to both Presidents Bill Clinton and George W. Bush. He now focuses his energy on warning against computer-based terrorism attacks. In his book, Cyberwar: The Next Threat to National Security and What to Do About It, he describes frightening scenarios where hackers could cripple the United States with a few clicks of a mouse. Clarke also chairs Good Harbor Consulting, a strategic planning and corporate risk management consulting firm.

“*For once it would be nice for the US to be able to be out in front of a catastrophe, to prevent that catastrophe,*” said Clarke. “*We know how to do it we just need to spend the money*.”

And the money is flowing. A whole cottage industry has sprung up around cybersecurity. According to Informationweek, the U.S. government is expected to spend $10.5 billion a year on information security by 2015. And Reuters reports that the worldwide market is as high as $140 billion a year. Cybersecurity is also one of the few areas in the new White House budget that escaped spending cuts.

And that, according to cybersecurity expert Dr. Sean Lawson, is the crux of the problem.

“*It’s going to become more common for defense contractors to hype cyber threats because that’s one of the few strains of money that still exists,” said Lawson, who also works as a contributor for Forbes Magazine. “It is a classic case of trying to motivate a response by rallying the troops by appealing to fear, by appealing to uncertainty.*”