Cyber attack equals act of war according to Pentagon

by Kismo *Tuesday, May 31 2011, 11:36am*
international / mass media / commentary

> The US, by threatening hackers with conventional military 'missile' responses, has indirectly admitted it lags far behind elite hackers in cyberspace. An ossified Pentagon imbecile is quoted in the Wall Street Journal as saying, "*If you shut down our power grid, maybe we will put a missile down one of your smokestacks;*" how very characteristic, a typically rustic, primitive, American response that only a banjo-playing moron would make openly – 'no doubt' the hacker community is packing shit!

I would defer to a piece in Forbes, which explains why this strategy is absurd, notwithstanding the US looks for ANY excuse to wage permanent war.

The simple facts are that a hacker's most important weapon is his/her ability to REMAIN INVISIBLE/undetectable/untraceable/anonymous. Elite hackers are only known by their many aliases never by face or orthodox methods of identification. Another feature of an elite attack is that it only becomes known AFTER the event!

It must be difficult for orthodox militarists to even imagine operating in a digital world where skill and agility/speed in real time is everything. How many times have intrusions been made with system administrators conducting daily maintenance tasks completely unaware that there precious systems have been compromised?

Now the Pentagon, after the hilarious and embarrassing attempt by the USAF to recruit hackers via conventional job advertisements, is THREATENING the hacker world with missile strikes!

Well, good luck Jethro, you have no idea how many of YOUR systems are already compromised; how they were compromised and by whom! Characters like Lamo and Assange are glory seeking, flawed personalities NOT elite hackers by any stretch. An elite hacker would never jeopardise his/her FREEDOM by going public. Julian Assange is a very good example of what not to do; he is currently under house arrest facing extradition; he must report to police daily and wear an electronic locating device (ankle bracelet) at all times – the price of notoriety!

Forbes report follows:

> **Crimes No One Can Stop -- Attackers No One Can Find**
> by John Mariotti
>
> If a thief were invisible, he might be able to steal at will and never be caught. How would anyone catch him? No one would know what he looks like. What could you look for? Next imagine groups of malicious vandals that cannot be seen . . . or found. How can you stop them? Can anyone stop them? Owners of Sony Play Station gaming systems are wondering that right now. Sony's CEO, Howard Stringer sounded a pessimistic note, commenting that he wasn't sure how to stop such invasions in today's cyber-threat filled world.

Media reports confirm this grave uncertainty about what to do:

The US has demanded a global response to the threat from cyber crime and cyber terrorism. The Obama administration wants to impose an international set of security standards, including penalties for nations and organisations that fail to comply, according to a report in the New York Times. The report added that White House officials hope that the strategy would prompt China and Russia to better control cyber crime in their own countries.[1]

Hope is the key word in the paragraph above, because "hoping for solutions" is all anyone is doing much of these days. These simple metaphorical questions describe the dilemma of dealing with cyber-crime and cyber-terrorism. There may be telltale traces of the crime, but these usually don't point back to any specific enemy. There is no way to counter-attack if you cannot find who attacked you, or how, or where they are. Many speculated that either the USA or Israel were behind the Stuxnet attacks on Iran's nuclear installations, but proof—that's not so easy to find. The Chinese have been suspected for the past ten years of being behind many of the worm virus attacks, notably the Conficker worm—one of the worst. But no one has absolutely proven anything.

Though it is not often headlined in the news, cyber-crime is something many people should be concerned about, "The continued rise of organized cyber-criminal gangs and the emergence of targeted advanced malware threats are the most concerning trend we've seen," said Dan Hubbard, CTO at Websense. Malware is defined as programs that are intended to do harm, and hackers, or "organized cyber criminal gangs," are people who try to "hack" into systems to alter them, either mischievously, or maliciously.

The conclusion of the United Nations Brief: "The Prevention of Cyber-Terrorism & Cyber-War" is not very comforting, because it reaches similar conclusions about cyber-attacks and cyber-crime:

"In sum, until the U.N. issues an effective international treaty to combat cyber crime, states, businesses and individuals have to protect themselves from cyber-attacks. This is nearly impossible as cyberspace is too large, too sophisticated and too interconnected to be dealt with alone without cooperation. Therefore, it is time for governments to sit together and formulate a single solution to this top concerning problem at the international level."

The trouble with this conclusion is that few believe any "treaty" will inhibit cyber-terrorists or cyber-criminals. They don't operate by such "rules." Instead, they laugh at them, and then hack into the sites describing the new agreements, disrupting them, to show their contempt.

However, experts around the world are puzzling over this challenge constantly, and some solutions are emerging. According to Matt Jonkman, founder of Emerging Threats Pro, some existing security strategies are effective against cyber-terrorism:

IDS (Intrusion Detection Systems)
IPS (Intrusion Protection Systems)
Antivirus, anti-malware, and anti-spyware software and hardware
Regular third-party testing

Other experts strongly recommend a multi-faceted approach. Keep existing security measures in place and up to date; use the most secure networks possible; make sure firewalls are “on,” use passwords that are robust and changed often, assure that virus protection is completely up to date, (because virus writers are constantly changing their invasion methods and places), and so forth. For example, virus writers are now creating viruses that morph, changing just a little bit of their code to avoid detection by anti-virus programs that looks for “signatures”—small sequences of coding that are common to a given kind of virus. When a little bit of that signature changes, does the anti-virus scan pick it up or not? It depends on how “little” that modification is.

These warnings are intended to make you aware of the huge, imminent threat presented by malware and hackers. When these hackers are many in number, the problem multiplies. “Crowd sourcing” gathers many hackers together electronically and aims them at the same target. This has become a popular form of attack. A report out of Dubai disclosed that al-Qaeda has combined the global reach of the Internet as a cyber-terrorism tool to influence and win over non-Arab sympathizers. Many believe that the Russian government used “crowd sourcing” attacks to shut down the nation of Estonia—a former Russian province—to show the Estonians that they were not really independent of Russia quite yet.

The largest problem is when a nation-state—is the perpetrator of cyber-terrorism. As noted previously, China has long been blamed as the source of the nastiest worm viruses (e.g., Conficker), which is reported to have infected tens of millions of computers. China is the alleged source of Ghostnet, an attack on Tibet, which infected 1200+ important systems in over 100 countries.

The problem is that no one can yet identify these crimes or prove the actions of the criminals. They cannot “see them” or “trace them” with enough certainty to stop them, apprehend (or counter-attack). Worse, some invasions leave “back doors” through which the perpetrators can easily “re-enter.” Even if the victim cleans them out, at some time in the future, they reappear as if by magic.

We have come full circle to the original dilemma. How do you stop a criminal you can’t see, or prevent them from committing a crime you can’t trace? The answers, thus far, are more conjecture than certainty. The threats are real and imminent.

[1] http://www.computing.co.uk/ctg/news/2071333/global-cyber-security-strategy

http://tinyurl.com/42og6yy
