Cyberweapons: Bold steps in a digital darkness?

Cyberweapons: Bold steps in a digital darkness?

> In the world of armaments, cyber weapons may require the fewest national resources to build. That is not to say that highly developed nations are not without their advantages during early stages. Countries like Israel and the United States may have more money and more talented hackers. Their software engineers may be more skilled and exhibit more creativity and critical thinking owing to better training and education. However, each new cyberattack becomes a template for other nations — or sub-national actors — looking for ideas. Stuxnet revealed numerous clever solutions that are now part of a standard playbook. A Stuxnet-like attack can now be replicated by merely competent programmers, instead of requiring innovative hacker elites. It is as if with every bomb dropped, the blueprints for how to make it immediately follow. In time, the strategic advantage will slowly fade and once-esoteric cyber weapons will slowly become weapons of the weak.

Source

There's a lot going on in this article. There's a huge amount going on in the background outside the article's sphere.

The article goes to lengths to point out without saying it point blank, that cyberweapons is now to replace the chemical warfare as poor countries future weapon of mass destruction. Depending on the circumstances and design, it may not be one of killing people but rather of making them uncomfortable and generally being one of annoyance while others are seeking the good stuff from secure sites. The cost is minimal compared to developing a nuclear bomb, delivery methods, and then storage and maintenance costs that endure as long as the weapon exists.

What isn't said and isn't even considered is the direction of present political forces in the US and what it's effects will be on this latest news that acknowledges the US's involvement in Stuxnet.

First off, the news that the US was involved, not as an accusation but as acknowledgement, means that the US will never have decent diplomatic ties with countries like Iran. Diplomatic ties are necessary to resolve conflicts and were I Iran I wouldn't be trusting the US after this. The US has already stated it considers cyberwarfare to be an act of war. So read here that the US's unclaimed stance is that it is at war already with Iran.

My next point is that recently, political forces in the US have been claiming that education, along with social benefits needs cutting but at the same time, the worlds largest army needs more funding. The military's job is to go in and break things and kill people after all negotiations have ended with no results.

In education it has been considered that STEM as it is called is the most important subjects to be taught and the US is failing miserably at it. STEM means Science, Technology, Engineering, and Mathematics; the basis for advancing knowledge and new developments in all fields. Politics got involved in education and what has resulted from President Bush's 'No Child Left Behind' program is that the teachers are being graded for job performance by classroom test scores. (Read job performance as keeping your job) So what is now being taught, isn't STEM, it's how to pass the test so I keep my job, that is being taught. At the same time, state funding for schools are being strangled as state funding hits record lows from the long term recession/depression. Where this will show up is in about 25 to 30 years from now when these who are now students become tomorrow's work force. You can't do STEM related work with out STEM related education. When you look at things like Creationism being politically mandated to be taught in school, without it having to pass the same criteria as science based, it gives you further clues to the future of advanced STEM education.

The programers that wrote these malware programs are all older professional programers according to the reverse engineering that was done and what was used and how it was used. Their professional life as a programmer will be ending within the next decade or two at best. At that time the question becomes who will take their place to provide national security for the computer operations that will continue to drive the economic well being of the nation.

It is no accident that the US has recently been hollering about needing national defenses for cyberwar. Mainly because they carry the knowledge they started it and must now protect themselves from their Frankenstein creation.

Share this:

- Share