White Paper:
Cyber Hawk or Digital Dove

SkillBridge

Published By: SkillBridge, LLC
September 18, 2013

Today's Modern Warfare

With the recent debate over whether or not the United States should take military action in response to chemical weapons being used against innocent civilians in Syria, one thing has become certain - The American people at this point in time have little appetite for offensive minded, physical military engagement.

Overwhelmingly, polls from every side of media show that this military action is unwelcome. "Boots on the ground" is the eventuality feared by both left and right wing opponents of a Syrian conflict. "No boots on the ground" is the promise our leaders make as they assure us that any military involvement will not put the men and women of our armed forces in the line of fire.

However, one question that has not been asked is how the American public feels about a different kind of campaign – one that does not involve soldiers on the front lines, but programmers using lines of code.

What was once considered futuristic science fiction, Cyber warfare is now today's reality. Whether in the form of unmanned drones controlled by an operator thousands of miles away from a target, or viruses that travel that same distance in a nanosecond, like it or not, the cyber domain is the next war front.

To some this may still seem like an idea that is better left for the pages of a 5 cent comic book. In reality, short of a nuclear attack, cyber warfare can do far more damage in far less time than the unleashing of traditional military might. Attacks on a nation's communications systems, energy networks, food supply chain, and other critical infrastructure have the potential to do catastrophic damage beyond what many could ever comprehend.

The severity of this threat can be underscored by the recent announcement of a new UK based think tank developed to study this very issue. Some of Britain's leading minds, including Lord Rees of Ludlow, past President of the Royal Society, Cambridge cosmologist Stephen Hawking, and Lord May of Oxford, a former government chief scientist, have launched "The Cambridge Centre for the Study of Existential Risk".

The Centre's effort includes the drafting of a "Doomsday List". One of these primary catastrophic events believed to hold the potential to threaten civilization as we know it (i.e. to bring about the extinction of the human species) is a wide scale cyber attack.

The bottom line, with the world's increased reliance on technologically interconnected networks, society as a whole is more vulnerable than ever.

For some nations Cyber warfare is an opportunity to level the playing field. The Syrian Electronic Army, while not identified as a direct vassal of the Syrian government, has wreaked havoc on Western targets, claiming credit for attacks against numerous Western news outlets and the US Marines recruitment website.

China is widely believed to be directly involved in attacks against multiple US companies, stealing vast sums of proprietary information and technology.

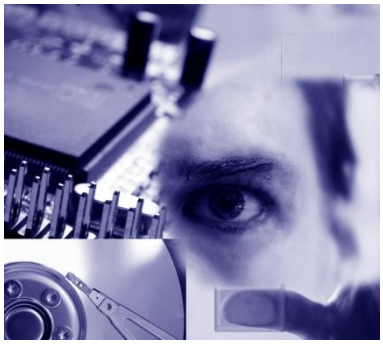
Israel and the United State are commonly understood to have been behind the Stuxnet attack that targeted Iran's Natanz nuclear facility, a watershed moment in Cyber warfare as a "proof of concept" attack, vividly demonstrating SCADA command and control system vulnerability.

As loosely affiliated rogue players and nation states alike proliferate their cyber warfare capabilities, a philosophical and strategic question for the United States becomes one of how to best approach the cyber front. Should the United States take an offensive of defensive posture as our enemies build their digital arsenal?

Simply put, do we invest our energies and resources into offensive strategies in the cyber arena, or do we focus on building our defenses to "keep the bad guy out"? This is actually equal parts philosophical and strategic as it is a question of resource allocation.

Do we invest our energies and resources into offensive strategies in the cyber arena, or do we focus on building our defenses to "keep the bad guy out"?

How to Build Our New Army



Whatever your preclusion may be, offensive or defensive minded, in the new world of cyber warfare, the real question we need to be asking ourselves is whether or not the United States is a Cyber Hawk or a Digital Dove.

It is well documented and understood that the United States is vastly undermanned in terms of well trained cyber security talent. Whether one prescribes to an offensive or defensive posture in this next field of battle, one particular point is glaringly obvious - the United States needs more ***cyber soldiers***.

Sweeping measure must be implemented, both the private and public sectors, to address this growing cyber security personnel deficiency. The most effective way to begin the process is to build threat awareness at every level of every organization. When it comes to cyber security, the "Not my job" mentality is no longer sufficient. For the entire Cyber Security chain to be effective, it is imperative that Cyber Security become everyone's responsibility.

In Cyber Security awareness training, the key to success is to quickly engage the participants, not only by demonstrating that the subject matter is pertinent, but that it directly applies to them.

This is accomplished by having the participants understand exactly what is at stake, both for them as individuals, as well as for the organization at large. For the general employee, this may mean that their job is on line. For the executive, the threat may be to the company's standing, reputation, and long term viability. For critical infrastructure organizations or government agencies, it may very well mean the safety and security of our nation's citizens.

Regardless of whether or not you are in the offensive of defensive camp, one other thing is clear. For the United States to be well positioned for prosperous, long term viability in this new cyber world, we need to start proactively drafting and training Cyber Soldiers at every level.

About the Author

Steve Leventhal is a partner in SkillBridge, LLC, a leading provider of Cyber Security training solutions for government and private industry.

SkillBridge's mission is to enhance enterprise security by providing targeted cyber security training that strengthens employee technical skills, processes, strategy, and user implementation in each distinct job role.

www.skillbridgetraining.com