

SECURITY DEBRIEF

www.securitydebrief.com



Scott Weber

Cyber Warfare & the United States – A Call to Arms

January 30th, 2009- by Scott Weber

U.S. Ambassador to the United Nations Susan Rice and the Obama Administration should press the United Nations to join the 21st century and address head on the issue of cyber warfare.

Article 51 of the U.N. Charter provides that a country has the right to engage in self-defense when it suffers an armed attack. The extent of such a response is guided by the Geneva Conventions and their attendant protocols, which define, among other things, the ways that a war may be fought and the protection of individuals.

These protocols also provide measures that can be taken to prevent or end “grave breaches,” defined as “willful killing, torture or inhuman treatment . . . willfully causing great suffering . . . and extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly.”

But what about cyber warfare?

When the laws of war were written in the Geneva Conventions in 1949, and even in the protocols that followed in the 1970s, the possibility of a cyber attack was not part of the arsenal of warfare. Today, however, cyber warfare is a very real and powerful threat.

Just prior to Russia’s deployment of tanks and war planes into the former Soviet Republic of Georgia in the summer of 2008, cyber attacks were reported as having been perpetrated by Russian state-run businesses against Georgia. Internet traffic was blocked, and Georgian web pages turned spoof, featuring misinformation and propaganda.

In December 2008, there was a cyber attack on a U.S. military classified computer network. The attack led the Pentagon to ban the use of external hardware devices because that was the source of the breach. Although it is not publicly known if this attack was “state sponsored,” media reports attributed the attack to either the government of China or Russia. Regardless of who perpetrated the attack, there was little that the U.S. could do to respond.

The question that must be asked is what redress exists in the international community to deal with state sponsored cyber warfare? The answer to this question is quite simple: none, because there is no international rule of law that expands the laws of war to cover cyber-attacks.

The U.N. should not wait for a cyber attack of epic proportions – on par with 9/11 – to mobilize the international community. Indeed, a major cyber attack could be more destructive than a conventional attack, as the affects of such an attack could literally shutdown the target country's government and ruin its economy. As a result of the interdependence of the world economy, the cascading affect would be felt worldwide.

The Obama administration should bring this issue to the forefront of its U.N. agenda and prompt the international coalition to address the reality of cyber warfare and its potential debilitating consequences. Warfare must be viewed in a new way because the old definitions and framework are impermissibly limited.

First, we must derive a definition to determine when a cyber attack is an act of war. Second, we need a broad definition of whom (including individuals, nations and groups) can be held accountable for such acts. Based on the current framework, only States may become parties to international treaties. Currently, almost all the world's States (192 to be exact) are parties to the Geneva Conventions. So the Geneva Conventions and its Protocols are enforceable simply by virtue of a State's membership. However, one dilemma involving cyber warfare is that its perpetrators are not necessarily states, but may be terrorist groups. International law ought to specifically include terrorist groups and organizations. Finally, a method of redressability, or punishment, for such acts must be determined.

As the Obama administration looks to instill change and meet the demands of a new age, it should press for the U.N. to meaningfully address the issue of cyber warfare. The U.N.'s condemnation of "terrorism in all its forms and manifestations" is insufficient. The United Nations must work to deter countries and their insurgents from engaging in cyber warfare and provide a forum and means to punish those who do. This will likely be a protracted process and, therefore, we cannot in the meantime let our guard down.

<http://securitydebrief.adfero.com/2009/01/30/cyber-warfare-the-united-states-a-call-to-arms/>
©2008 Adfero Group. All Rights Reserved.