John Pires

SE 4930

December 09, 2011

Article Review 1: Cybermilitias and Political Hackers

Summary

The purpose of this article is to provide background and information on what the author terms "cybermilitias", as well as discuss the various pros and cons of utilizing them. A cybermilitia is defined as "a loose confederation of hackers conducting cyberattacks under the overt or covert direction of a nation-state against another nation-state to further the strategic, political, or military objective of the initiating state." Governments will devote sections of their military to cyber warfare, but this article deals with the pros, cons and logistics of non-state cyber warfare entities.

Normal civilians cannot just pick up a rifle, go halfway across the world, and wage war against a country; any attempt to do this on a large scale would either be squashed by the civilian's home country, or if endorsed, be an obvious and overt act of war. In the modern age however, anyone with access to a computer is capable of committing acts of war through cyberspace. There are many "hacktavist" groups in existence and a large number of attacks have been carried out by such groups. These attacks can be motivated by politics, beliefs or simple patriotism. The idea of a cyber militia is for a government to influence or even directly control these groups.

Cyber warfare lends an entirely new face to war in general. Cyberspace attacks are subtle, difficult to track, difficult to prove, shadowy and obscure in every aspect. If one country were to launch a single missile into another country and cause a very small amount of damage the attacking country would receive worldwide condemnation and perhaps even instigate a war. However, if that same country were to launch a cyber attack which caused far more damage the attack would most likely result in nothing more than speculation and debate. Furthermore very few of the established international definitions and rules concerning war can be applied to hackers conducting cyber attacks and defense. A combatant can no longer be defined as a uniformed soldier, carrying a gun, under direct control of an officer. Another compounding factor is that every remotely attackable military target would make large-scale use of civilian resources and infrastructure so it would therefore be logistically impossible to completely separate military targets from civilian resources.

This incredible level of uncertainty in both defining and even proving/detecting attacks is what makes dealing with cyber attacks such a difficult problem. The article also states that even if proper definitions and rules could be created and internationally agreed upon the effort would ultimately useless as the lack of accountability would mean no one would follow them. To illustrate this point the article includes the following quote by Stewart Baker, former General Counsel for the National Security Agency: “It is a near certainty that the United States will scrupulously obey whatever is written down, and it is almost as certain that no one else will.”

The article ends with an analysis of the pros and cons of utilizing cyber militias. Numerous pros are listed for using cyber militias as a tool for attack. Attackers have a clear and decisive advantage as they gain the initiative immediately, choose the exact time and place of their attack, determine the scale, and are “shielded by the legal ambiguity generated by a lack of applicable international laws covering cyber warfare”. The only drawback listed is the difficulty in controlling a cybermilitia. For instance, it could be difficult to halt an attack, or overly ambitious hackers could attack sensitive civilian targets such as healthcare facilities which would result in immense political backlash if detected and proven. The article ends with the conclusion that cybermilitias are here to stay and will play a large role in future warfare. There are very many advantages to using them, not the least of which being that poor, or militarily weak, countries can utilize them. Other countries, specifically China and Russia, are already aggressively developing information warfare programs which utilize cybermilitias and the United States must formulate a response, one way or another.

What was learned

I learned quite a bit about cyber warfare in general and the logistics behind it. It was very interesting reading about the problems in trying to apply conventional military rules to something like cyberspace. Additionally I knew that cyber warfare is a real thing but I had no idea that cyber militias are such a big part of it.

The article was very non-technical so not much was learned that can be directly applied to secure software development. However, I did learn a new term, obfuscation, which is the hiding of intended meaning in communication, making communication confusing, willfully ambiguous, and harder to interpret. This is applied in software development to make code more difficult to read and thus more difficult to understand and/or reverse engineer. Despite being non-technical the paper did give me new ideas and considerations to apply to software development. For instance, the idea that civilians (foreign and domestic) could attack my system in response to some political stimuli or belief structure must be

taken into account. Also, if my software or system is running in a way in which it is associated with a potential military target or is on the path to gaining access to a military target additional security must be used.

I thought of several questions I would like to answer while reading the article. They mostly concern large scale and general topics. I would like to know the full scale of cyber warfare and how much and how often is being used. I would like to know what branches of the United States military deal with cyber warfare and defense and what their overall strategy is. Unfortunately it is unlikely I will ever get complete answers to these questions due to their sensitive nature, but it is very interesting.

Works Cited

Applegate, Scott. "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare." *IEEE Security & Privacy Magazine* 9.5 (2011): 16-22. Print.

"Obfuscation." *Wikipedia, the Free Encyclopedia*. Web. 14 Dec. 2011. <http://en.wikipedia.org/wiki/Obfuscation>.