Dan Bednar
Article Review 1
12/11/11
Cyberwarfare
From IEEE Security & Privacy

The article talked about how software could be used in warfare. One thing it pointed out was that software could be used to attack others by non-governmental (non-state) groups. A good chunk of the article was discussing how non-state groups were taking their own initiative to use software to damage property or otherwise disrupt government function.

The first part of the article talked about attacks in the past. These were attacks that I had never heard of. Growing up it was this kind of thing that interested but instead of attacks we just heard of viruses. Even in my adult life I didn't hear anything and I was more news conscious then. Like the Chinese patriotic group attacking Iran after an Iranian group hijacked a Chinese search engine.

I remember the conflict that Russia had with Georgia back in 2008. What wasn't reported was the denial of service attacks that Russia did to Georgia. This leaves me wondering what would happen to the United States if an attacker did a DoS attack to our government in middle of an engagement. There does not appear to be an easy answer to that question either. At least, none is offered by the report.

Another part of the article focuses on how software has caused, or is alleged to have caused damages to physical property. The computer guy in me finds it fascinating that a piece of code could cause a pipeline explosion or disable centrifuges at a nuclear enrichment facility. The pipeline example from 2010 is particularly interesting to me. From what I've seen and hear of this in other classes it sounds like the application was originally designed by a normal company with no desire for that kind of functionality. It appears that a government created a worm to change the behavior that caused the centrifuges to become damaged.

The software engineer in me sees a huge problem with that however. The application used was not secured enough to prevent a worm from changing its behavior. Programmed properly by engineers there is no way this should have happened. Of everything in the article, it is this that I must learn from. If I ever work on something that isn't supply chain and do something that controls big machinery or really anything to do with manufacturing.

The Rest of the article focused on how civilians are engaging in what the author describes as acts of warfare. The fact that civilians are able to organize and pull off these feats with such relative ease shows the need for better programming practices in the way of security. In the case of the software that ran the centrifuges the code wasn't exactly public knowledge. Only by ignorance or mistake could something that closed off and limited in availability to the public or other governments be compromised. Like the Therac 25 is to an example to the need of good design, reviews and testing, the centrifuges are for security.

The article itself was a good look into how many groups of people can and have used software for cyberwarfare and done so on many occasions. It left two questions open though. The first question is what would happen today if someone attempted to do a DoS attack against the Russians, Chinese or even the US? More importantly, how can these be prevented? The examples and short sorties were great examples on how bad things can be but there were never any "lessons learned" mentioned or even ways to help lessen the probability of attack later.