Week 08 Writing Assignment

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

A Brief Analysis of Russian Cyberwarfare Capabilities – Past, Present, and Future

Matthew Crosston, Ph.D. - Professor

October 21, 2012

Information provided in the November 2011 Potomac Institute for Policy Studies set of lectures on Russian Cyber Capabilities was an excellent, authoritative indoctrination for understanding the mindset of the Russian leaders toward cyberwarfare, as well as understanding the history and foundation of these perspectives. Specifically, it showed that Russian leaders frame their cyberwarfare capabilities and ideas under the idea of Information Security of the Russian Federation. Analysis of their mindset and activities reveals the following:

- Putin is indeed very tech-savvy
- The Russian military has successfully waged punishing cyberwar operations against both Estonia and Georgia
- The mindset of the Russian leaders is often described as a "19th century geopolitical perspective"
- The Russian people are still unhappy with the outcome of the fall of the Soviet Empire, which is regarded as the greatest geopolitical failure of the 20th century
- The Russian leaders and its military have the will and the capability to wage cyberwar if necessary to achieve whatever national political objectives are deemed as necessary for the benefit of the Rodina (The Motherland)
- Regarding their own people, Putin's Information Security Doctrine of September 2010 empowers the state to control information to accomplish these objectives:
  - Protect strategically important information
  - Protect against deleterious foreign information
  - Inculcate patriotism and values

(The Potomac Institute for Policy Studies, 2011).

Though it has not been widely publicized, as far back, as 1982 and again in 2000, the Russians were themselves attacked by cyberattacks in the control systems associated with their remote Siberian gas pipelines (2011, Tsang).

As mentioned earlier, the punishing Russian cyberattacks on Estonia in 2007 and Georgia in 2008, demonstrated an effective and visible cyberwarfare capability not previously witnessed, and ironically there was no attempt to conceal these (Czosseck and Geers, 2009).

In the article, ***Russia Now 3 and 0 in Cyber Warfare***, it was revealed that apparently, in January 2009, Russia launched its third massive set of DDoS cyberattacks on Kyrgyzstan, which is also one of its neighbors. So in each of the years between 2007 and 2009, Russia showed that it was able, willing, and very capable in conducting effective cyberwarfare operations to achieve their desired military and national objectives in the cyberspace shared with its neighbors (Carrol, 2009).

In 2009, it was also noted that Russia and the U.S. have fundamental disagreements on what the nature of treaties should be to prevent cyberwarfare. At that time, Russian leaders, recognizing the reportedly favored a total cyberweapon disarmament. The U.S. vehemently disagreed with this position, stating that it was necessary to concentrate on strong cyberdefensive capabilities due to the fact that they were seeing as many as 50,000 attacks per day (Markoff and Kramer, (2009). It became clear at this time that the inability for these two “cyber superpowers” to reach an agreement on the use of cyberweapons would likely result in a cyberweapons arms race and increase the danger and possibility of a cyberwar.

Yet, as late as 2011, specific cyber capabilities of what the Russians either currently possess or are in the process of developing became publically known. Despite official denials to the contrary, Russian documents were obtained and translated. These documents show that there is active research on development of cyberattack tools and capabilities in the following areas:

- "Means of effect on components of electronic equipment and its associated power supply
- Temporary or irreversible disabling of components of electronic systems
- Means of power electronic suppression: ultra-powerful microwave generators
- Explosive magnetic generators
- Explosive magneto-hydrodynamic generators
- Software for disabling equipment (hard drive head resonance, monitor-burnout, etc.
- Software for erasing rewritable memory
- Software for affecting continuous power sources
- Means of disabling electronic networks
- Means of effect on programming resource of electronic control modules
- Disabling or changing the algorithm of functioning control system software by using special software
- Means of penetrating information security systems
- Means of concealing information collection sources

- Means of disabling all or specific software in information systems, possibly at a strictly given point in time, or with the onset of a certain event in the system (i.e. a logic bomb)
- Means of covertly partially changing the algorithm of functioning software
- Means of collecting data circulating in the enemy information system
- Means of delivering and introduction of specific algorithms to a specific place of an information system
- Means of effect of facility security systems
- Means of effect on programming resource of electronic control modules
- Stopping o rdisorganizing the functioning of data exchange subsystems by an effect of the signal propagation medium and on the algorithms of functioning
- Electronic warfare assets, especially ground-based and airborne (helicopters and unmanned aerial vehicles)
- Droppable expendable jammers
- Means of effect on the data transfer protocols of communications and data transfer systems
- Means of effect on addressing and routing algorithms
- Means of intercepting and disrupting the passage of information in its technical transfer channels
- Means of provoking a system overload by false requests of establishing contact (i.e. DDoS attacks) (K, 2011)"

This extensive specific list of areas of research made me think that perhaps some Russian hackers were behind the massive power grid failures that affected the Northeastern part of the United States in August 2004. Certainly, if their capabilities were advanced enough in 2004, they could probably have undermined infrastructure defenses in the U.S. to successfully execute such an attack, possibly simply as a show of force and/or to probe our capabilities to defend against and respond to such an attack.

After seeing the extensive list of potential and current cyberweapon capabilities, it became clear to me that Russia intends to dominate cyberspace if they are given that opportunity by the U.S. failing to recognize and meet the threats.

By 2012, analysis by an Israeli defense analyst showed the following regarding Russian policy and strategy related to cyberweapons:

Country	Policy	Strategy
Russia	Russia supports cyberwarfare capabilities, especially providing such capabilities in the Russian Army. The nature of cyberwarfare and information warfare requires that the development of a response to these challenges must be organized on an interdisciplinary basis and include researchers from different branches – political analysts, sociologists, psychologists, military specialists, and media representatives (Fayutkin, 2012).	The ability to achieve cyber superiority is essential to victory in cyberspace. (Fayutkin, 2012).

So what does it all mean? Obviously Russians have progressively demonstrated that they have the will, the vision, the doctrines, the tools, the knowledge, and experience with which to successfully wage serious cyberwarfare. Russia is now and should be regarded for the foreseeable future, as a potential and worthy adversary, and it should be considered to me "cyberweapon superpower" on the battlefield of cyberspace.

References

Carrol, W. (2009). Russia Now 3 and 0 in Cyber Warfare. Retrieved from http://defensetech.org/2009/01/30/russia-now-3-and-0-in-cyber-warfare/ on October 21, 2012.

Czosseck, C. and Geers, K. (Editors) (2009). The Virtual battlefield: Perspectives on Cyber Warfare. Washington, DC: IOS Press.

Fayutkin, D. (2012). The American and Russian Approaches to Cyber Challenges. Defence Force Officer, Israel. Retrieved from http://omicsgroup.org/journals/2167-0374/2167-0374-2-110.pdf on September 30, 2012.

K., Dr. (2011). Hacker's Handbook, fourth edition. London, U.K.: Carlton.

Markoff, J. and Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. An article published in the New York Times on June 28, 2009. Retrieved from http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all on June 28, 2009.

The Potomac Institute for Policy Studies. (2011). Russian Cyber Capabilities: Policy and Practice. A conference video posted at YOUTUBE.com. Retrieved from http://www.youtube.com/watch?v=ZVwVhegU1S4&feature=related on October 19, 2012.

Tsang, R. (2009). Cyberthreats, Vulnerabilities, and Attacks of SCADA Networks. A scholarly paper published at the University of California at Berkley. Retrieved from http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf on October 21, 2012.