Week 07– Writing Assignment 03

William Slater

DET 630 – Cyberwarfare and Cyberdeterrence

Bellevue University

Strategic Comparative Analysis in Cyberwarfare and Cyberdeterrence

Matthew Crosston, Ph.D. - Professor

October 14, 2012

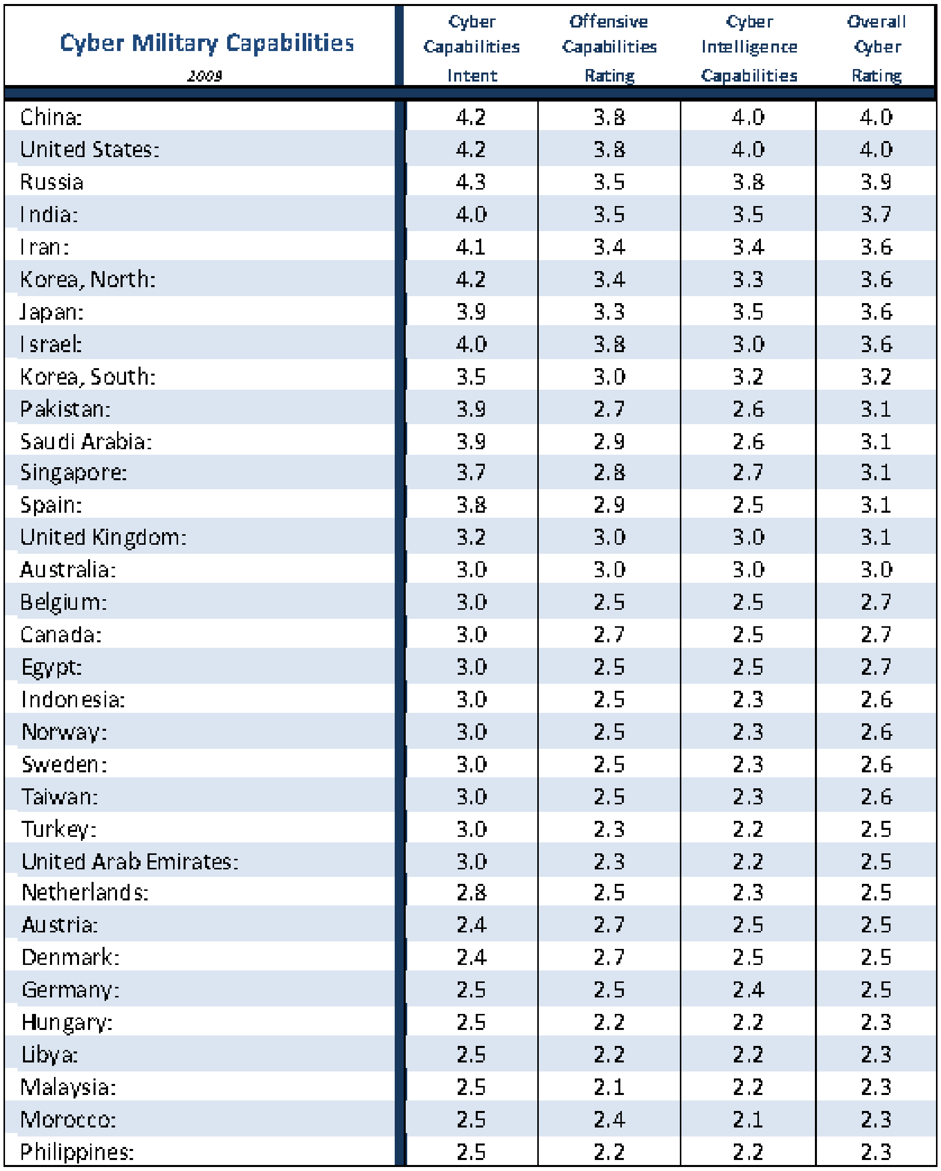
Strategic Comparative Analysis in Cyberwarfare and Cyberdeterrence

This brief paper will present a strategic comparative analysis of the present state of cyberwarfare and cyberdeterrence issues.

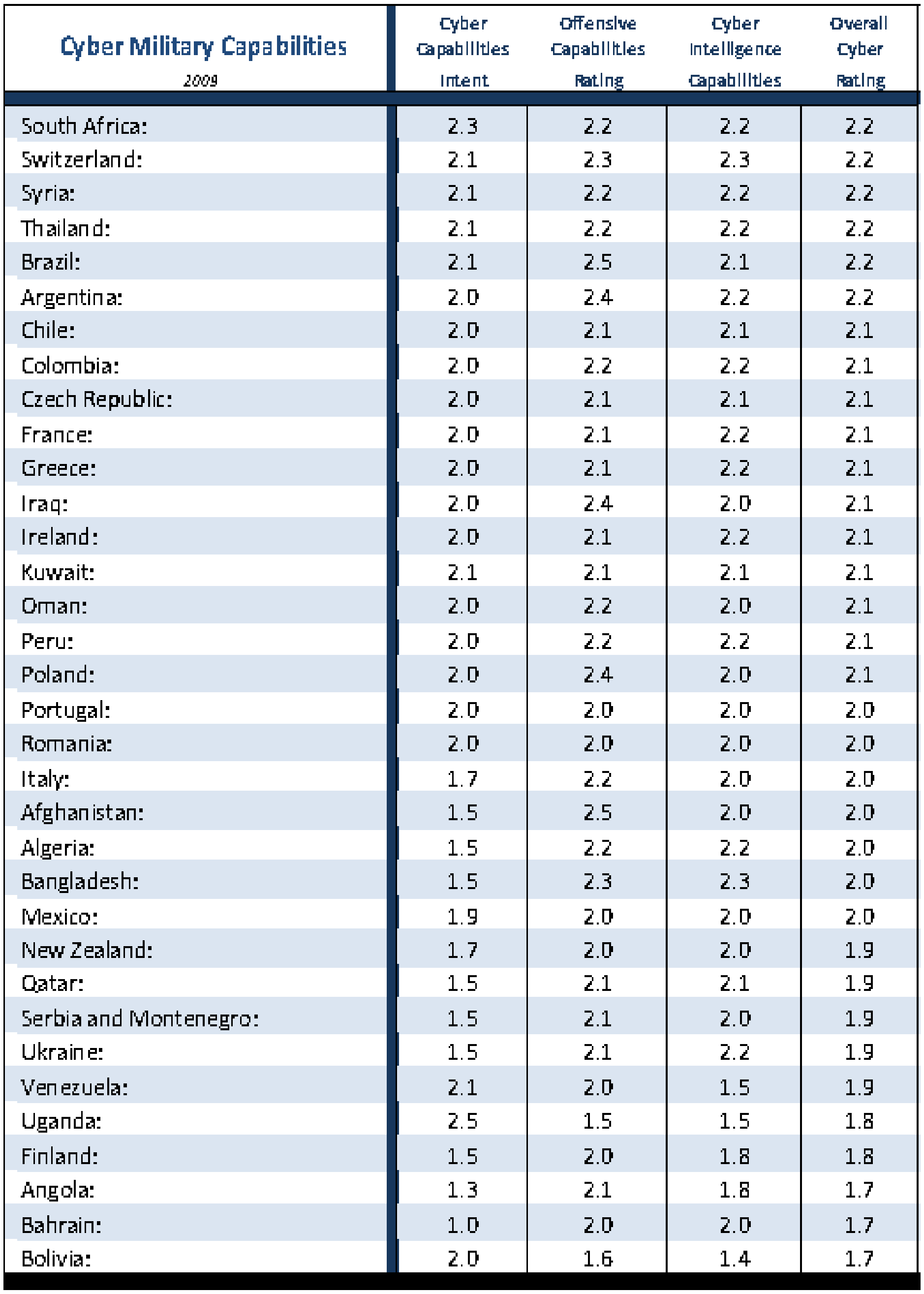
What Other Countries / Regions of the World Are Concerned with This Same Threat Issue?

The countries that are primarily concerned with cyberwarfare and cyberdeterrence threat issues are the same countries that already have the greatest cyberwarfare capabilities and also the most to lose in the event of a full-scale cyberwarfare attack.

The diagram below from 2009 shows the comparative cyberwar capabilities of the 66 largest countries in the world.



Cyber Military Capabilities 2009	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China:	4.2	3.8	4.0	4.0
United States:	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India:	4.0	3.5	3.5	3.7
Iran:	4.1	3.4	3.4	3.6
Korea, North:	4.2	3.4	3.3	3.6
Japan:	3.9	3.3	3.5	3.6
Israel:	4.0	3.8	3.0	3.6
Korea, South:	3.5	3.0	3.2	3.2
Pakistan:	3.9	2.7	2.6	3.1
Saudi Arabia:	3.9	2.9	2.6	3.1
Singapore:	3.7	2.8	2.7	3.1
Spain:	3.8	2.9	2.5	3.1
United Kingdom:	3.2	3.0	3.0	3.1
Australia:	3.0	3.0	3.0	3.0
Belgium:	3.0	2.5	2.5	2.7
Canada:	3.0	2.7	2.5	2.7
Egypt:	3.0	2.5	2.5	2.7
Indonesia:	3.0	2.5	2.3	2.6
Norway:	3.0	2.5	2.3	2.6
Sweden:	3.0	2.5	2.3	2.6
Taiwan:	3.0	2.5	2.3	2.6
Turkey:	3.0	2.3	2.2	2.5
United Arab Emirates:	3.0	2.3	2.2	2.5
Netherlands:	2.8	2.5	2.3	2.5
Austria:	2.4	2.7	2.5	2.5
Denmark:	2.4	2.7	2.5	2.5
Germany:	2.5	2.5	2.4	2.5
Hungary:	2.5	2.2	2.2	2.3
Libya:	2.5	2.2	2.2	2.3
Malaysia:	2.5	2.1	2.2	2.3
Morocco:	2.5	2.4	2.1	2.3
Philippines:	2.5	2.2	2.2	2.3



Cyber Military Capabilities *2009*	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
South Africa:	2.3	2.2	2.2	2.2
Switzerland:	2.1	2.3	2.3	2.2
Syria:	2.1	2.2	2.2	2.2
Thailand:	2.1	2.2	2.2	2.2
Brazil:	2.1	2.5	2.1	2.2
Argentina:	2.0	2.4	2.2	2.2
Chile:	2.0	2.1	2.1	2.1
Colombia:	2.0	2.2	2.2	2.1
Czech Republic:	2.0	2.1	2.1	2.1
France:	2.0	2.1	2.2	2.1
Greece:	2.0	2.1	2.2	2.1
Iraq:	2.0	2.4	2.0	2.1
Ireland:	2.0	2.1	2.2	2.1
Kuwait:	2.1	2.1	2.1	2.1
Oman:	2.0	2.2	2.0	2.1
Peru:	2.0	2.2	2.2	2.1
Poland:	2.0	2.4	2.0	2.1
Portugal:	2.0	2.0	2.0	2.0
Romania:	2.0	2.0	2.0	2.0
Italy:	1.7	2.2	2.0	2.0
Afghanistan:	1.5	2.5	2.0	2.0
Algeria:	1.5	2.2	2.2	2.0
Bangladesh:	1.5	2.3	2.3	2.0
Mexico:	1.9	2.0	2.0	2.0
New Zealand:	1.7	2.0	2.0	1.9
Qatar:	1.5	2.1	2.1	1.9
Serbia and Montenegro:	1.5	2.1	2.0	1.9
Ukraine:	1.5	2.1	2.2	1.9
Venezuela:	2.1	2.0	1.5	1.9
Uganda:	2.5	1.5	1.5	1.8
Finland:	1.5	2.0	1.8	1.8
Angola:	1.3	2.1	1.8	1.7
Bahrain:	1.0	2.0	2.0	1.7
Bolivia:	2.0	1.6	1.4	1.7

Table 1 – Country Cyber Capabilities Ratings (Technolytics, 2012)

Countries Regions of the World That Do Not Place a High Priority on This Threat Issue

Countries that are more focused on the survival and welfare of their citizens, coupled with the fact that they are largely consumers of Internet and computer capabilities versus being able to afford to channel resources into the development of cyberweapons or the resources required to develop a credible cyberdeterrence strategy. It is also ironic that the U.K. with its stature and status does not rank higher on the list shown in table 1.

Some of the Current Policies Being Employed by These Other States / Regions in Regards to the Threat

China, Russia, and India, each of which are in the top four of the countries listed in Table 1, have well-defined cyberwarfare policies and strategies. Ironically, the U.S., which occupies the number 2 position in that same table, does not yet have well-defined cyberwarfare policies and strategies. For comparison, Table 2 below shows a summary of the policies and strategies of China, Russia and India.

Country	Policy	Strategy
China	China supports cyberwarfare capabilities, especially providing such capabilities in the People’s Liberation Army.	The Chinese will wage unrestricted warfare and these are the principles: Omni-directionality Synchrony Limited objectives Unlimited measures Asymmetry Minimal consumption Multi-dimensional coordination Adjustment, control of the entire process (Hagestad, 2012).

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).
India	India supports cyberwarfare capabilities, especially providing such capabilities in the Indian Army. "It is essential for efficient and effective conduct of war including cyber-war. The war book therefore needs to specify as how to maintain no-contact cyber war and when the government decide to go for full-contact or partial-contact war then how cyber war will be integrated to meet overall war objectives (Saini, 2012)."	Strategies are still under development, but will follow the guidance of policies related to the conduct of war. (Saini, 2012)

Table 2 – Summary of Cyberwarfare Policies and Strategies of China, Russia, and India

Successes and Failures of the Various Alternative Policies Around the Globe

Despite some of the negative press from the Stuxnet virus, this collaborative effort by the U.S. and Israel has been looked at with both fascination and as an event that has quickly and successfully heralded in a new age of warfare, the age of cyberwarfare. However, many still feel that in the absence of publically defined policies and strategies by the Obama Administration, it invites a secretive and even random appearance of and the continued use of cyberweapons (Sanger, 2012).

Areas of Joint Communication / Operation / Cooperation that Exist or Should Exist Across Countries Dealing with This Threat Issue

Apparently, the U.S. has already created cyberweapons with the help of Israeli cyberweapon experts. At least one of these cyberweapons was effectively used to impede the development of Iran's nuclear material refinement program from 2009 to 2010.

It is likely however, that through the auspices of the United Nations, or perhaps some G20 accord, there may be some general consensus on the importance of defining the appropriate uses cyberweapons. There also needs to be some agreement on types of response to cyberattacks, and effective methods of cyberdeterrence.

Is There One State in Particular That Seems to Be Doing a Better Job Than the United States Related to Dealing with This Threat Issue?

China is probably doing a better job than the realm of cyberwarfare for three reasons: 1) the government has invested considerable resources into their cyberwarfare capabilities; 2) the number of personnel devoted to cyberwarfare efforts is reportedly in the tens of thousands; and 3) the Chinese government is able to easily operate under a cloak of secrecy and conduct operations without fear of cyberwarfare activities being leaked to Chinese press agencies.

Recommendations for the U.S.

In August 1945, the dramatic destruction of both Hiroshima and Nagasaki not only resulted in the surrender of Japan and effectively ended World War II, it ushered in the age of nuclear warfare. Yet, it was years until the U.S. had the policy and unified strategic plan, the SIOP, with which to centrally control the use of nuclear weapons in wartime situations, as well as conduct a national policy of strategic nuclear deterrence.

It is not unreasonable to assume that the path towards a cohesive U.S. policy and set of strategies regarding the use of cyberweapons will follow a path that is similar to the strategic war plan maturity path from Hiroshima to the SIOP. Today, in the absence of any clear policy on the use of cyberweapons, Crosston advocates the agreement on a policy of "Mutually Assured Debilitation" in which everyone with cyberweapons would come to a general understanding that the use of these weapons would result in the expectation that massive destruction would be unleashed on every participant's assets (Crosston, 2011). This makes perfect sense considering that the "Mutually Assured Destruction" nuclear deterrence policy was effective and worked well during the Cold War from the 1950s to 1980s.

Yet, today, I believe that once a cohesive U.S. policy on cyberwarfare and cyberweapons is defined by the National Command Authorities, there is an eight-step process that could result in the development and rapid maturation of a strong national strategy U.S. Cyberwarfare:

1) Define the doctrines and principles related to cyberwarfare and the needs under which cyberwarfare would be conducted.
2) Create the policies that embody these doctrines and principles.
3) Conduct the intelligence gathering to accurately understand the landscape of the cyber battlefield.
4) Perform the analysis to create the strategy
5) Create the strategic plan and tactics

6) Conduct regular war games, at least twice yearly to test the strategic plan and tactics
7) Analyze and document the results of the cyberwarfare war games.
8) Refine the strategies and tactics for cyberwarfare and cyberdeterrence based on the results of analyzing the outcomes of the cyberwarfare war games

Note that it is also essential to continually assess the capabilities of Information Technology so that tools that our cyberwarfare fighters are using are state of the art and that they are effective and perform well as they are integrated into the cyberwar war fighting environment.

Conclusion

This paper has presented a brief strategic comparative analysis of countries with cyberwarfare capability and presented a set of processes by which the U.S. can quickly catch up where it is lagging behind in policies and strategies that will define its ability to conduct cyberwarfare and cyberdeterrence in the future.

References

Carr, J. (2012). Inside Cyber Warfare, second edition. Sebastopol, CA: O'Reilly.

Crosston, M. (2011). World Gone Cyber MAD: How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence. An article published in the Strategic Studies Quarterly, Spring 2011. Retrieved from http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf on October 10, 2012.

Czosseck, C. and Geers, K. (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.

Hagestad, W. T. (2012). 21st Century Chinese Cyberwarfare. Cambridgeshire, U.K.: IT Governance.

Hyacinthe, B. P. (2009). Cyber Warriors at War: U.S. National Security Secrets & Fears Revealed. Bloomington, IN: Xlibris Corporation.

Kaplan, F. (1983), The Wizards of Armageddon: The Untold Story of a Small Group of Men Who Have Devised the Plans and Shaped the Policies on How to Use the Bomb. Stanford, CA: Stanford University Press.

Kramer, F. D. (Ed.), et al. (2009). Cyberpower and National Security. Washington, DC: National Defense University.

Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: Rand Corporation.

Saini, M. (2012). Preparing for Cyberwar - A National Perspective. An article published on July 26, 2012 at the Vivikanda International Foundation. Retrieved from http://www.vifindia.org/article/2012/july/26/preparing-for-cyberwar-a-national-perspective on October 14, 2012.

Sanger, D. E. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of America Power. New York, NY: Crown Publishers.

Technolytics. (2012). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict, third edition. Purchased and downloaded on September 26, 2012.