

Admiral William A. Owens, Kenneth W. Dam, and Herbert S. Lin:
Understanding Cyber Attack as an Instrument of U.S. Policy

National Strategy Forum Event Summary

By Eric S. Morse

Admiral William Owens, Kenneth Dam, and Herbert Lin addressed the National Strategy Forum and the Chicago Council on Global Affairs at the Chicago Club on January 28, 2010.

The world is a complex information society intricately laced across globe-spanning computer networks. Cyber threats make America's way of life vulnerable to disruption, and at worse, systemic breakdown. Our society functions largely on technology, and that technology is vulnerable to attack. State and non-state actors are investing in the technological capabilities to carry out cyber attacks. Iran, China, Russia, and North Korea are known state culprits; the others are individuals and small groups, about which less is known. The common thread is their intent to use cyber attacks against American targets.

Given the threats that we face from state and non-state actors, it is worth considering how the U.S. might use its vast technological resources for development of offensive cyber operations.

Developing and implementing offensive cyber attack capabilities requires a robust discussion about the costs and benefits, both domestically and internationally, of this foreign policy tool. For example, the ramifications of using cyber attacks against an enemy may amplify the ongoing "cybernetic arms race."

Most people are familiar with cyber security defenses. These commonly impact our daily lives in the forms of firewalls, personal passwords, virus protection programs, and other measures. Offensive cyber capabilities, the action(s) taken by an individual or a government to harm computer and technological infrastructure, is a new, emerging field in national security.

Information on defensive security measures are easier to come by. Information about offensive cyber capabilities is usually classified, making it much more difficult for the academic and policy community to engage in the discussion about appropriate use.

The goals of U.S. offensive cyber policy, according to the Department of Defense, is the superiority and dominance of cyberspace. However, developing a working system is more complicated. Issues for the policymaker to consider include:

- Rules of engagement
- Training regiments for "cyber soldiers"
- Civilian privacy policy & protection
- Organizing an offensive Cyber Attack Center
- Preparing a list of likely targets to guide development of offensive capabilities

The Q&A discussion provided several insights. First, when asked if the Chinese government was responsible for the recent Google cyber attack, Admiral Owens responded that he did not

think it originated from the Chinese government, and noted that Google was not profitable in China (compared to Baidu, the competing search engine). Second, when asked if the U.S. could narrow the list of potential cyber adversaries to prepare against, the panel responded that this would be difficult because cyber attacks/intrusions are very difficult to trace electronically. Finally, when asked about productive political interaction on cyber policy, the panel suggested that the U.S. and China would mutually benefit from a cyber treaty in which both countries would agree to not attack the other.