PacNet
Number 41A

Pacific Forum CSIS
Honolulu, Hawaii

July 16, 2012

A Plea for an Alliance-Based 'AirSeaCyber' Joint Operational Concept

by Harry J. Kazianis

Harry Kazianis [harry@the-diplomat.com] *is Assistant Editor for The Diplomat and a non-resident fellow at the Pacific Forum: CSIS. The views expressed in this article are those of the author and do not reflect the position of The Diplomat or Pacific Forum.*

In PacNet #41, Mihoko Matsubara correctly asserts that "countering cyber threats demands cooperation among nations, in particular public-private partnerships." Cyber war has finally made its way onto the radar, and rightly so. Now the United States military must integrate cyber considerations into its new AirSea Battle concept.

US Secretary of Defense Leon Panetta warned that the "next Pearl Harbor we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems." If true, cyber must be front and center in any military refocusing to the Asia-Pacific. Any failure to not correctly plan against this lethal form of asymmetric warfare could be a catastrophic mistake.

The US seems to be focusing the military component of its widely discussed 'pivot' to Asia on China's growing military capabilities. While neither side seeks confrontation and one hopes none will occur, China's development of a highly capable Anti-Access/Area Denial (A2/AD) battle plan to deter, slow, or deny entry into a contested geographic area or combat zone has been detailed extensively. Cyber war is clearly part of this strategy, with Chinese planners prepared to wage 'local wars under conditions of informatization,' or high-intensity, information-centric regional military operations of short duration. Prudent military planners must be prepared to meet this potential threat. Other nations such as North Korea and Iran are also developing A2/AD capabilities with cyber based components that could challenge US or allied interests.

In this type of threat environment, the US, along with its allies, should develop its own symmetric and asymmetric counter-strategies. A joint operational concept of AirSea Battle that includes a strong cyber component would give US forces and their allies the best chance to defeat adversary A2/AD forces. Of course, the current Joint Operational Access Concept does make strong mention of cyber operations. However, an even stronger emphasis on cyber warfare is needed. In short, AirSea Battle as an operational concept might already be obsolete and it should be reconstituted as an "AirSeaCyber" concept.

If cyber is to become a full-fledged component of AirSea Battle, its conceptualization and integration are crucial. A simple first step must be the recognition that cyberspace is now one of the most important battlefield domains in which the US and allied militaries operate. It is not enough to exercise battlefield dominance in a physical sense with technologically advanced equipment. With vital but vulnerable computer networks, software, and operating systems a potential adversary may choose an asymmetric cyber 'first-strike' to damage its opponent's networked combat capabilities. Enemy forces could attempt to 'blind' their opponent by crippling computer and network-centric command and control (C2), battlefield intelligence gathering, and combat capabilities by conducting advanced cyber operations. Simply put: US and allied forces must fully understand and articulate the severity of the threat they face before they can map out any national or multinational strategies.

Working with potential cyber allies to identify common threats and working to mitigate possible challenges is crucial. One viable partner in creating effective cyber capabilities is South Korea. Seoul faces a number of problems from a growing North Korean asymmetric threat in a physical sense, as well as multiple challenges in cyberspace. General James Thurman, US Forces Korea Commander, recently noted that "North Korea employs sophisticated computer hackers trained to launch cyber infiltration and cyber-attacks." Pyongyang utilizes cyber capabilities "against a variety of targets including military, governmental, educational and commercial institutions." With the US committed to South Korea's defense, creating partnerships in cyberspace can only enhance such a relationship. Both sides must look past physical threats and expand their partnership across this new domain of possible conflict.

Japan is another possible cyberspace partner. As Matsubara accurately points out, "They [US and Japan] have more to lose. If cyber-attacks and espionage undermine their economies or military capability, larger geostrategic balances may be affected and the negative consequences may spill over to other countries." Both nations have reported hacking incidents from Chinese-based hackers that have targeted defense-related industries and programs. With Japan and the US partnering on joint projects such as missile defense and F-35 fighter jet, the protection of classified information associated with these programs must be a top priority. As military allies, both must plan for possible regional conflict where cyber warfare could be utilized against them.

Sadly, restraints could develop that might hamper such partnerships. One recent example: historical and political tensions have delayed and possibly halted a defense agreement between Japan and South Korea. The pact would have assisted in the direct sharing of sensitive military information concerning North Korea, China, and missile defenses. Presumably, cyber-related information would have been at the center of such sharing. The agreement was supported by Washington, which has been working to reinforce trilateral

cooperation with the two countries, as essential Asian allies. With all three nations facing a common challenge from North Korea, such an agreement would have been highly beneficial to all parties.

If other nations' military planners rely heavily on asymmetric warfare strategies, US planners and their allies must also utilize such capabilities in developing their response. Cyber warfare offers proportionally the strongest asymmetric capabilities at the lowest possible cost. Almost all military C2 and deployed weapons systems rely on computer hardware and software. As other nations' military planners develop networked joint operations to multi-domain warfare, they also open their systems for exploitation by cyber-attack. US and allied technology experts must begin or accelerate long-range studies of possible adversaries' hardware, software, computer networks, and fiber optic communications. This will allow US and allied cyber commands to deploy malware, viruses, and coordinated strikes on fiber-based communications networks that would launch any enemy offensive or defensive operations. Cyber warfare, if conducted in coordination with standard tactical operations, could be the ultimate cross-domain asymmetric weapon in modern 21st century warfare against any nation that utilizes networked military technologies.

Any good operational concept must always attempt to minimize any negative consequences of its implementation. AirSeaCyber presents US policymakers and their allies with a toolkit to deal with the diverse global military challenges of the 21st Century. The inclusion of cyber obviously declares that the US and its allies are prepared to enter a new domain of combat operations. This focus could unnecessarily draw attention to a domain that should be left to 'fight in the shadows' to avoid engendering a new battleground with deadly consequences. Some argue that with the use of cyber weapons against Iran to degrade its ability to develop uranium enrichment technology, a dangerous new international norm – operational use of cyber weapons – is upon us.

While these arguments have some validity, cyber war, whether against corporations, nation-states, or even individuals, is now part of daily life. To not prepare fully for this eventuality means facing battlefield obsolescence. Any student of history knows the results of preparing for the wars of years past-likely defeat.

These are only a sample of capabilities that could be utilized to create a joint operational concept that transition from present AirSea Battle ideas into a more focused AirSeaCyber operational concept. Such notions are compliant with current fiscal realities, utilize modern military technologies, and can leverage existing alliance networks. Any operational concept that will guide US armed forces in the future is obsolete without intense conceptualizations of cyber warfare. Working with allies to develop ties in cyberspace in the Asia-Pacific can only create a strong force multiplier effect and should be considered a top priority.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed.