Chinese Use of Cyberwar as an Anti-Access Strategy

Two Scenarios

MARTIN C. LIBICKI

CT-355

January 2011

Testimony presented before the U.S. China Economic and Security Review Commission on January 27, 2011

RAND
CORPORATION

Published 2011 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Martin C. Libicki[1]

The RAND Corporation

Chinese Use of Cyberwar as an Anti-Access Strategy
Two Scenarios[2]

Before the U.S. China Economic and Security Review Commission

January 27, 2010

Good afternoon, and thank you for inviting me here. I am Martin Libicki, from the RAND Corporation. I've been thinking about how states might use cyberwar for strategic purposes for most of the last twenty years.

Based on that, what I would like to do is to illustrate some of the strategic choices facing China and the United States in cyberwar by generating two scenarios and seeing where they lead.

In the first scenario, Taiwan shuffles towards independence. China concludes that it will have to take the island. It believes the United States may come to Taiwan's defense, but might be pressured into staying home. So thinking, China launches a wide-scale *strategic* cyberattack on the U.S. power grid, throwing the Midwest into the dark. Their message to us: do not delude yourself that the costs of intervention will occur only in our side of the world. Your citizens will suffer directly. Stay home.

But would such a strike do what it was intended to do? A cyberattack would have a coercive effect only if we could attribute the attack to China. Therefore, assume as much. Following the cyberattack, China then invades Taiwan. Will the United States be inhibited from intervention? Based on our reaction after Pearl Harbor and 9/11, probably not. Moreover, the Chinese, who take history seriously, would likely believe as much also.

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT355/.

Worse from the Chinese perspective is the likelihood that such an attack would change the narrative of the conflict in ways they would not like. Prior to the cyberattack, the Chinese could make the following case: "*Taiwan is part of China. Its separate status is an artifact of history. China is only rectifying the past to restore the nation's historic sovereignty. Taking Taiwan does not mean that China has designs on Japan, South Korea, the Philippines, or Southeast Asia – which are clearly different countries."* But once the lights go out here, the United States will be perceiving a different narrative being sent from China: "*China is rising and the United States is falling. The United States dare not intervene in China's part of the Pacific because it fears being hurt*." A cyberattack, therefore, changes any cross-Straits conflict from a local matter to a global matter. If the United States does not step forward – particularly if it looks as though the cyberattack scared the United States government – it will reinforce this second narrative and our fabric of mutual alliances in Asia will be rent. So, the United States intervenes for *strategic* reasons.

If the Chinese understand as much – and they very well might – they will conclude that a strategic cyberattack is a very poor coercive tool and its application may well backfire.

Now let us look at a seemingly similar – but far different scenario. Taiwan makes a move towards independence. China decides it is time to take the island. In contrast to the previous scenario it concedes that the United States *will* intervene on Taiwan's side. So, China takes steps to complicate and hence delay the U.S. transit of the Pacific, so that by the time the United States does arrive, the war will be over, or at least the Chinese will have a secure lodgment on the island. So, they carry out a full-fledged *operational* cyberattack on United States military information systems with the hopes of turning data into unusable nonsense. My former colleague, James Mulvenon, testified before your Commission that the Chinese might corrupt the time-phased force deployment data accessible through the United States Department of Defense unclassified Internet. Although the Chinese may also have other targets, concentrating on that database suffices for our purposes.

Would that make more sense from China's perspective? Yes. Such an attack is directly relevant to how the United States carries out military operations. To the extent that the United States uses force – which the Chinese already assume will take place – a cyberattack on such a force is a legitimate use of power. Furthermore, it is by no means clear that such a cyber-attack offers a narrative, as a *public* challenge of the United States would. The workings of U.S. military logistics may not be secret but they are esoteric to almost all of the U.S. public. It is entirely possible that such an attack never hits the news (at least not until after the after-action analyses take place).

If such a cyberattack were to take place *after* Chinese forces had begun irrevocable moves towards Taiwan, and if the fact of U.S. intervention was already determined, then the U.S. military would have little choice but to deploy anyway and work around the disruption or corruption of its databases as best as it could.

However, under this second scenario now consider the possibility that the Chinese are holding back while waiting to see how badly U.S. forces have been stymied by the cyberattack. If it received indications – perhaps visible but more likely gathered from listening posts the Peoples' Liberation Army (PLA) may already have within unclassified defense networks – that the hoped-for effect has taken place, then the PLA may conclude that it has achieved a favorable correlation of forces and goes ahead. If, however, the hoped-for effects fail to materialize then perhaps the correlation of forces is not so good and they stand down and deal with the fallout from the cyber-attack later, perhaps by denying everything.

From the U.S. perspective, if it suffers just such a large scale operational cyberattack (and no war has started), its first challenge has to be to answer the question "is there a war coming soon?" Why "soon"? Because the effects of such a cyberattack are temporary (if no hardware has been broken); the window of disability is relatively small, measured in days. If a war is to take advantage of the interim confusion, it will likely start within such a time-window. Conversely, if some preparations for war have been discovered but no war has started, the next challenge for the U.S. military is to project that its ability to operate has been unaffected, the better to tilt China's decision in favor of staying put. The third challenge is to actually get better. Fourth and last is to worry about how to respond to the cyberattack itself – which, if a war does start, would be quite low on the priority list since responding to their invasion will be primary.

Would a cyberattack on U.S. forces actually work to degrade mission effectiveness? I don't know. Unfortunately, it is not clear whether anyone else does, either. If the military knew the specific vulnerabilities that such an attack would exploit, then one would think they would have been fixed by now. The Chinese, alone, may know what they, themselves, are capable of. We, alone, may know where our weak spots are. Neither of us is sharing information with the other on the topic.

But, determining whether such a cyberattack would work may be a secondary question. More critical is whether the Chinese *think* that they can alter the correlation of forces with a cyberattack on the U.S. military. If the answer is yes, and they find themselves debating whether to go to war, their confidence may impel them towards going ahead (incidentally, a similar argument can be made for outer space). In such a case, if they carry out a cyberattack and it turns out that the United States *can* fight its way through it with little effect, then although U.S. forces will be in a better position to fight, war will have begun anyhow.

Therein rests the challenge for the U.S. military: first, to determine to what extent its ability to carry out its missions is at risk from *any* cyberattack; second, to ensure that it has the resiliency to fight through cyberattacks; and third, to make everyone else, not least of which is China, aware of how well it can withstand attack. In January 2011, the Secretary of Defense said that “Chinese technological advances in cyber- and anti-satellite warfare posed a potential challenge to the ability of our forces to operate and communicate in this part of the Pacific.”[3] That suggests that the third task has not yet been accomplished, perhaps because the second task remains unfinished as well. Unfortunately, it is by no means clear that we have undertaken the first – understanding what the risk to our mission effectiveness from cyberwar *is*.

These are not impossible tasks. The oft-stated aphorism that cyberspace is a man-made medium means that the United States Department of Defense can make its networks into what it will – and do so in ways that nullify temptations to mischief that our weaknesses would otherwise engender.

My conclusions are twofold. First, that the threat of *strategic* cyberwar is probably overblown. Second, that the United States Department of Defense needs to take the prospect of *operational* cyberwar seriously enough to understand imaginatively and in great detail how it would carry out its missions in the face of a full-fledged attack.

[3] Pomfret, John. “Regional risks making U.S. - Japan ties even more key, Gates says” The *Washington Post*. Washington D.C.: January 14, 2011. pg. A 10.