

*Blown to Bits: China's War in Cyberspace,
August-September 2010*

We encourage you to e-mail your comments to us at: strategicstudiesquarterly@maxwell.af.mil .

Reader's Comments

From Rick:

Computerworld carried a story by Christopher Bronk written for *SSQ* on [What a cyber war with China might look like](#). Since my general mode of interaction with people is to leave them better than I found them, I offer some humble observations. I use the word 'humble' because I am, after all, a novelist playing with fictional constructs. Mr. Bronk deserves acknowledgement of his serious work.

1. In the last paragraph of page 4, a statement is begun, "While the goal is not to get bogged down on the particulars of why such a conflict would come to pass..." Wow, talk about ignoring the real global reality! The myriad possible scenarios yield as many ways such a cyber war would manifest itself. In fact, a reasonable topology of the "whys" motivating a cyber war would then yield a corresponding set of response scenarios that could not only nip cyber war in the bud but which could generate the cyber equivalent of M.A.D. (Mutually Assured Destruction) publicly stated doctrines....The absence of such publicly stated doctrines indeed invites and makes cyber war inevitable....

2. In the first full paragraph on page 6: "But in the days running up to the war, that activity spiked enormously." In my mind, this is unlikely that China would telegraph the first moves of an all-out cyber war. That would be downright stupid. Just like Pearl Harbor, the Japanese goal was to take out the biggest part of our Pacific fleet in a surprise attack. Again on page 9: "The cyber attack had a rolling start, rather than being a bolt from the blue." Pure balderdash.

3. Interestingly, two paragraphs later the characterization of a "...small piece of data, only 256 bytes long..." accurately describes the behavior of one of many probes possible....Perhaps it's because he didn't want to give our cyber enemies any new ideas. Unfortunately because of this constraint, this picture of cyber war is rather one dimensional.

4. Page 8's scenario of a Chinese defector waltzing "...into the Australian consulate in Tokyo..." is entertaining, since I believe Australia will play a major role in world cyber security....Only they don't know it yet.

5. On page 10: "...Guam was the sole location of an electromagnetic strike by the Chinese..." In a full-blown cyber war, EMP weapons make excellent sense in multiple locations. Especially in hardened locations tuned for retaliation and defense actions at the outbreak of cyber war.

6. Mr. Bronk's depiction of our reaction to the ways in which the Chinese wage this war is again one dimensional....

7. On page 16 Mr. Bronk makes a compelling case for cyber privateers. He says the FBI will lead the charge "[e]nlisting the hacker community..." in the effort. I believe this is wrong minded, using coercion to recruit versus using monetization of the process to licensed and bonded entities. I hope this blog and my arguments will correct a fearful misdirection of effort.

8. On the next page, again Mr. Bronk builds a case for a new paradigm, since "decisions by conference" is a doomed idea. Unfortunately, the closest convergence to my cyber privateering idea comes on page 18: "Civil defense in the cyber domain must be considered a necessity."

9. Finally, Mr. Bronk's paper does nothing whatsoever to deal with the specifics of our response to and strategies with which we will turn the tide and win the cyber war. In fact, it seems to assume that we will simply defend against the attacks until the enemy wears down and that we not mount our own overwhelming retaliation. How can you seriously suggest that this paper is a picture of our cyber war with China? I realize you don't want to telegraph our own playbook. But this paper is definitely not a picture of any kind of cyber war.

To the U.S. Air Force cyber defense brain trust, I beg you to distribute your brain power MIPS now and not wait until you're in the midst of a full-blown cyber war. Let's face it: Cyber war will be pretty well automated and occur in minutes and not days or weeks. The response must also be systematized and does not lend itself to a committee of men with lots of stars on their shoulders, especially if those military leaders must wait for step-by-step authorization from political leaders. And finally, we need stated doctrines that unambiguously detail our automated response to the nanosecond-by-nanosecond realities of cyber war (my point number 1 above). Not to do this pretty well guarantees a cyber Armageddon from which we will not be able to quickly rebuild.

From Michael:

I read your story, "[Blown to Bits](#)" and right from the beginning I kept asking myself why you were so focused on the importance of humans managing these cyber attacks. Why would you need 60,000 people??

The future battle will be fought by computers with a level of intelligence that allows them to attack based on their programmed business rules that define the attack game. Your focus on humans is surprising especially when you describe 256 bits of data that can self-evolve. If 256 bits can do so much then there is a high probability that a large computer could do much worse by generating its own snippets of code and sending them into the wild against their programmed enemy in a cross coordinated yet independent attack.

Of course this means that each country will have its own super computer attack system and they will all attack and defend in pico seconds. Imagine a 24 hour day where 3 million battles were fought and each super computer having its own scorecard of percentage of wins and losses. By the time our military reviewed the previous day's battle 3 million more battles would have been

fought. In fact the people in charge may no longer now exist because the enemy computer erased them from history in yesterday's battle.

This will bring society to the point they will realize there is no true defense to stop the enemy's offense. No level of firewalls or security systems will be effective against quantum computers. Which will cause everyone to conclude technology cannot be trusted by anyone for anything.

Soon after, technology will no longer need mankind, it will have evolved beyond our understanding and be able to support, enhance, and evolve on its own (based on your article). So in essence, our military objectives will have caused us to create something more powerful than ourselves, that no longer needs mankind, AND does not have a conscience because we programmed it to be a ruthless warrior that shows no mercy.

It's funny how today we act like a bunch of ants down on the pavement battling among ourselves and use our ingenuity to eventually cause our extinction.

If we don't care what life we step on as we walk down the street imagine how computers will treat us when we are no longer necessary.

From Noah:

The internet has always been a middle road between liberal and realist objectives. For liberal theorists the internet has been a collaborative means for free sharing of information to create improvements, and for realists the internet was created for national security purposes to ensure military communications would continue during a nuclear war. The Christopher Bronk article, *[Blown to Bits](#)*, featured in the Spring 2011 *[Strategic Studies Quarterly](#)* was on target with its implications for the future of cyberwar. The author goes to great depth explaining East Asian use of the internet and their government efforts to come to grips with the force of the internet, but does not mention the efforts by the US government and US businesses over the past couple years. In short, the social media giant, Facebook, has been an advocate for the future of the internet on their terms, and the current US Administration is supportive of their vision. The recent protests throughout the Middle East and North Africa and the respondent US efforts are the first test of this concerted policy, and will continue to shape the future of cyber reality....Believe it or not, social media led by Facebook is becoming the main tool for driving change in support of US objectives. As mentioned earlier, the internet has always been a middle road, but will the internet become The Silk Road? Referring to the Central Asian region where trade routes determined and oriented national strategies for control. Only time will tell what the outcome will be.