CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Cyber War and Competition in the China-U.S. Relationship[1]

James A. Lewis

May 2010

The U.S. and China are in the process of redefining their bilateral relationship, as China's new strengths means it has a new position and new responsibilities in the world. Cyber conflict could become a significant and damaging factor in this process of bilateral redefinition, as it involves and exacerbates both economic and military competition.

Why is there so much attention now to cyber security? We have discovered a new dependence on the global information infrastructure built over the last two decades. This infrastructure has become a new arena for competition, in part because it was never designed to be secure and in part because it is weakly governed.

We also need to consider cyber conflict as part of a larger change in the international security environment, as power flows away from Europe and as the legitimacy of the global institutions developed after world war two comes under question. A new, multipolar order is emerging but we do not yet know its outline or final shape.

American and Chinese beliefs and perceptions are important in shaping competition and our ability to manage it. For an outsider, the most influential elements in Chinese thinking appear to be a desire to develop asymmetric military capabilities, to promote indigenous innovation, and to restore China's rightful place in the world after the "Century of Humiliation." These factors are complicated by a new sense of China's power and uncertainty over how China's political process will evolve. For cyber security, China's complex and evolving attitudes towards intellectual property are also particularly important

On the American side there is discomfort with new vulnerabilities we perceive in our society, concern over the apparent erosion of American power, which I should note is due largely to internal political factors, uncertainty about China as a competitor, and a sense that new powers like Brazil, India and China will take advantage of the global economic system the U.S. helped to create.

These beliefs and perceptions mean that there is currently little room for cooperation in cyber security. This will not change without much more work in recognizing the scope of the problem. However, our actions can increase the possibility for cooperation, and I do not think conflict is inevitable if tensions can be managed for a period of years.

Cyber conflict is the focal point of these tensions, embodying as it does military competition and asymmetric warfare, barriers to trade, economic espionage, and the prospect for long term damage to both nations economies and influence. What has been a largely covert competition in cyberspace is now becoming overt.

[1] Remarks delivered at the China Institutes of Contemporary International Relations, May 13, 2010

Both nations face important decisions on how to adjust their policies to take into account the growing importance of the information infrastructure we call cyberspace. A key decision for the United States is how much longer to tolerate economic damage from cyber crime and cyber espionage, largely but not entirely the result of the theft of intellectual property and confidential business information. This is a difficult topic to discuss, but it is slowly gaining attention in Washington, particularly after the Google episode. The risk, of course, is that some unexpected event will change this slow-moving debate into crisis or conflict.

Key decisions for China include how to protect intellectual property in cyberspace in both China and in other countries, as weak protection will slow and damage indigenous innovation, China must find ways to accommodate the growing political power of China's "netizens," and decide whether to curtail the use of proxy forces in cyberspace.

Powerful misperceptions on both sides shape these decisions but there is one misperception we can clear away immediately. We are not in a cyber war.

War is the use of force to achieve political ends. It involves using force to attack, damage or destroy an opponent's capability and will to resist. A cyber attack would damage data and perhaps physical infrastructure, create uncertainty in the mind of an opposing commander, and be used for political effect.

In war, we can regard cyber as just another weapons system, capable of long range strikes at high speed. It will not be a decisive weapon, but its use will provide an advantage. Most advanced militaries have cyber attack capabilities and many other militaries are developing them.

Advanced militaries also have missiles and aircraft and plans to use them, but they will not use these weapons outside of a larger armed conflict. No one would launch a missile or an aircraft at the United States on a whim or as a test, as this would invite a devastating response.

If we get into an armed conflict, say with Russia over Georgia, I fully expect cyber attacks to be used by both sides. All advanced militaries have cyber attack capabilities and have conducted the reconnaissance necessary or attack in the event of war.

Even then, there are political constraints on the use of cyber attack. We sometimes hear that cyber attacks are like nuclear weapons. This is silly, but there are some similarities in the risk of escalation and in the political uncertainties cyber's use could bring.

In a cyber attack, we do not know the scope of collateral damage, that is damage to things other than the intended target. Computer networks are connected in strange ways. They have grown up like a coral reef or forest, without central planning, and guided only by the concerns of business and engineering.

This means we could attack one network only to find that the network of third parties depend on it. We could attack the telecommunications system of Iraq and find that this also damages allies or even ourselves. This uncertainty about is a constraint on some kinds of cyber warfare.

At the same time, cyber attacks risk the escalation of conflict. An attack on deployed forces is to

be expected, but an attack on critical infrastructure in the opponent's homeland risks a significant escalation. Cyber attack can easily change an armed conflict from a localized battle to a strategic engagement.

Asymmetry in cyber attack also risks escalation. An attack on critical infrastructure using cyber tools may invite a kinetic response. We should not think of armed conflict that includes cyber attacks as limited to hacker versus hacker. The U.S. term for this is "cross-domain" deterrence.

Pure cyber war, a war between two countries only involving cyber attack, is very unlikely. What would a nation gain from a series of relatively weak strikes on an opponent? Outside of a larger armed conflict, cyber war is unlikely.

This is not to say that we would not benefit from establishing how cyber war should be conducted or how the existing international laws of war apply to it or should be modified. If we wait until first use, it will be too late.

We do not have a framework for cyber conflict, a shared lexicon, or even a good ability to communicate about it with potential opponents, as the U.S. and Soviet Union were able to communicate about military activities during the Cold War. Developing this framework of norms and expectations for cyber conflict would improve international security.

One reason for this is that we face the eventual use of cyber attack by non-state actors, such as terrorists. My belief is that at the moment, they do not have the capability to launch cyber attack. If they did have the capability, they would have used it. The real question is how long will it take non-state actors to acquire these capabilities from the cyber crime black market. I believe this will happen in the next few years.

Developing a framework for armed conflict could reduce the changes of misinterpretation. The most important issues for this framework are thresholds, particularly deciding what is an act of war, and the application of existing international norms for conflict to cyberspace

That we are not in a cyber war does not mean there is no conflict in cyberspace. Cyberspace is the wild west, a lawless environment where crime and espionage are daily occurrences. The United States believes it is the primary target of crime and espionage, because of its wealth, its advanced technology, speed of adoption and because of the new competition we see in contemporary international relations.

Many nations – Brazil, India, Russia, the Europeans – along with the U.S. and China are vying for influence to reshape international rules and institutions to better serve their own interests. The term from game theory for this would be "zero sum game," a competition where for one side to gain, the others must lose.

The long term effect of this zero sum competition could be very damaging to global prosperity and security, and a key decision for new entrants like the BRICS is whether and when they will stop saying that the "global north," the developed countries, owe the "global south," and this debt justifies a zero sum approach. These countries cannot be forced to abandon this ideology, they must be persuaded that it is in their interest not only seek to gain advantage in the

international system but to also strengthen it in ways that are "non-zero sum," ways that provide benefits to all players.

I believe one reason for the stability of the system of laws, trade and financial rules created by the U.S. and its allies in the 1940s – a system that led to globalization and greater economic growth than had ever been seen before – is that it had this "non-zero sum" quality. The result is a collection of global networks for communication and travel unrivalled in history and enabled by key political decisions made decades ago.

No intellectual framework has emerged to replace this "Wilsonian" vision of the world, but that does not mean it is not being eroded. The continued failure of trade talks is the best example of this erosion and uncertainty over the future of cyberspace is another.

Nor is this to say that the U.S. is not motivated by self-interest. All nations are motivated to some degree by self interest. But U.S. policy has been consistent for more than a century in saying that the rule of law and an open global economy were in the best interest of the United States and of other nations.

It is interesting to note that this system was developed in response to the perceived failures of the 1920s and 1930s – the last time we saw multipolar competition; failures that led to global depression and war. The post war system sought to replace force and imperialism with the rule of law and to create a sense of equity in international relations.

Many developing countries, of course, believe that law has not replaced force and that international relations remain inequitable. I will tell you that many Americans are coming to believe that the same is true for cyberspace, and that it is time to respond.

When the Cold War ended, the U.S. did not expect to find itself in a new competition, one where technological leadership and the ability to innovate was more important than military strength, one where conventional military competition would be replaced by asymmetric warfare.

Information technology plays a central role in this new competition. In the last twenty years we have created a global infrastructure called cyberspace that has become an essential part of our lives. Global information networks connected national economies more closely than ever before. They accelerate research and innovation. But they have also become a source of vulnerability and a new venue for conflict.

The primary aspects of cyber conflict as it is waged now involve crime and espionage, including espionage conducted by proxies. These proxies are essentially cybercriminals or hackers acting at the behest of a government, as irregular forces or mercenaries

One reason cyber conflict has gotten out of control is that this information infrastructure is very weakly governed. The pioneers of cyberspace believed it would be a self-organizing community, open, non-hierarchical, where national borders would not apply and where governments were not needed. Perhaps this idea made sense in the past, but it does not make sense now and one fundamental question for all nations is how to extend sovereignty and the rule of law into cyberspace to reduce conflict in ways that do not damage or destroy this unique

infrastructure.

It is important to distinguish between conventional espionage and economic espionage in this new competition. All nations have agents who seek military and political information. This will not change and there are unspoken rules that apply to this. One problem for cyberspace is that we have been lax in applying these traditional rules for espionage.

However, economic espionage is different. It can be carried out by governments, but also by companies and even individuals. It is, in fact, better seen as a criminal activity. It is economic espionage that causes the greatest damage and this could easily become a flashpoint and a source of increased tension in the bilateral relationship.

For the U.S., the primary task is to build better defenses and, perhaps, find new ways to deter opponents. There are things the U.S. can do on its own to reduce the damage from economic espionage. We are now in our fourth effort in 12 years to improve our defenses. I think we will see finally some success.

It is too easy to overstate any possible U.S. vulnerabilities. I remember that in the 1970s, a Soviet General said that the correlation of forces had shifted irrevocably to the Socialist camp. He was not the first to make this mistake, since America's resiliency is easy to underestimate.

But creating a more secure cyberspace is not just in the U.S. interest nor will it benefit only the U.S. The U.S. must also find ways to work with new partners. As technology has diffused around the world, cyberspace has gone from having a single country as its architect to having many. Ensuring that these architects have a common vision that is consistent with human rights and dignity and that is also technologically effective is a new and important task.

There is much work that needs to be done to make cyberspace more stable and secure for all countries. I see this as a continuation of earlier efforts to create institutions and rules for a more stable global economic and security environment. This will require approaching the problem of cybersecurity on three levels: State-to-state conflict, both political and military; law enforcement, to reduce cyber crime; and trade, including IP protection, non-tariff barriers to trade, and competition over standards.

One persistent myth from the age of the cyber pioneers is that cyberspace is a global commons. This is wrong. There is no moment when the collection of networks and digital devices that make up cyberspace are not owned and subject to national sovereignty. Cyberspace is not a commons; it is a condominium where the owners lack good ways to cooperate.

Sovereignty in cyberspace is usually interpreted as the right to control the bits of information that flows into a country, but it must also include the responsibility to control the bits that flow out. The excuse that it was patriotic hackers is no longer acceptable.

I believe the goal for the international community is to develop shared understandings and principles on what is responsible behavior in cyberspace. This will require development of norms and agreements, perhaps accompanied by new institutions, perhaps modeled on ICAO or FATF.

I would like to suggest five areas where international cooperation would be beneficial.

The first is to determine to how to extend sovereignty into cyberspace without damaging connectivity and openness. Governments will play an increasing role in cyberspace, and we need to find ways to reduce the chances of harm or conflict.

The second is to develop principles and norms that define responsible state behavior

The third is to expand international governance for cyberspace, recognizing that a single overarching entity is probably a recipe for failure, and that any governance structure must not damage connectivity, openness and innovation. Effective governance is closely related to norms – value free governance will be ineffective.

A fourth area is to develop and apply rules for cyber conflict. This can help reduce the changes of misperception, overreaction and escalation. This could include tacit or unspoken understandings on thresholds, on what is an act of war, and what level and kind of response is appropriate for cyber attack.

Finally, we must extend equitable trade rules into cyber space, to protect intellectual property, to avoid a politicized standards process that will harm innovation, and to dismantle non-tariff barriers to trade. This is particularly important for the bilateral relationship.

None of these tasks will be easy, but they are also not impossible. Nations will have to decide how they will work together to modify or replace existing international structures and institutions and how these decisions will be applied to cyberspace.

I leave you with a fundamental question. Is our relationship in cyberspace a zero sum game or is there room for cooperation? My sense is that if we do not engage, this conflict which has so far been largely invisible, will only get worse.