Statement before the House Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, and Emerging Threats

Cyber Attacks:
An Unprecedented Threat to U.S. National Security

March 21, 2013

Michael Mazza
Research Fellow
American Enterprise Institute

Chairman Rohrabacher, members of the subcommittee:

Thank you for the opportunity to testify before you today on China's use of cyber capabilities and how the United States might respond.

The cyber realm is a relatively new one and thus one that we are still working to understand. Offensive cyber capabilities are particularly worrisome for a number of reasons. These unconventional weapons may be used by state or non-state actors and, when used, their origin may be difficult to trace. Appropriate responses to their use remain a matter of debate.

In some ways, the advent of cyber warfare calls to mind the early days of the Cold War, when there was little agreement on how nuclear weapons should be used. Were atomic weapons simply big bombs or did they represent a revolutionary capability, something new and different? Would they most effectively be used against civilian populations, conventional military targets, or the enemy's own nuclear weapons? Was it possible and affordable to defend against long-range ballistic missiles armed with nuclear weapons and, if so, would such defenses be stabilizing or destabilizing? It took decades of intellectual efforts from political scientists, economists, physicists, and others to satisfactorily address these questions, some of which are still debated today.

I raise this analogy for two reasons. First, the analogy suggests that we are only in the early stages of what will likely be a long-term effort to understand conflict in the cyber realm.

Second, while the role of nuclear weapons in national security has long been hotly debated, that debate did come to some consensus that those weapons are tools of statecraft—though perhaps controversial ones—and can be used as such. China, at least, appears to have reached the same conclusion about cyber capabilities. A first

order question, then, is: what are China's ends and how does it operate in the cyber realm to achieve them?

China's Rise and Cyber Statecraft

The primary objective of the Chinese Communist Party (CCP) is to stay in power. No longer securing its legitimacy on a foundation of Marxist ideology, the party now relies on delivering prosperity and its claim to a nationalist mantle to ensure its continued rule.

China has seen sustained, high levels of economic growth over the past two decades, with GDP growth in the high single- and low double-digit rates. As recently as 2007, China experienced 14.2% growth.[1] Growth has slowed somewhat since, with 2012's rate reaching a nadir of 7.9%, the lowest in 13 years.[2] Given the weaknesses inherent in China's economy—poor performing loans, weak domestic consumption, shoddy ownership rights, a shrinking labor force, to name a few—it will be difficult for the country to return to the high-charged growth of past years.

One reform that would help the Chinese economy would be to strengthen domestic intellectual property rights (IPR) protections and enhance enforcement. Such moves would help to spur innovation and make China a more attractive place for multinational corporations to do business. But such reforms still appear unlikely for several reasons, including:

1) There remain vested interests opposed to IPR enhancement.
2) China's relatively low position on the value chain does not lead to the creation of large constituencies in favor of stronger IPR.
3) It is easier to steal knowledge and technology than for China to develop it itself.

That third point is most relevant for our purposes. General Keith Alexander, Commander of Cyber Command and Director of the National Security Agency, has described cyber theft of U.S. intellectual property as the "greatest transfer of wealth in history," citing a cost to U.S. companies of approximately $250 billion per year.[3]

---

[1] "GDP growth (annual %)," The World Bank, http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG, accessed March 20, 2013.

[2] Kevin Yao and Aileen Wang, "China's economy posts slowest growth since 1999," Reuters, January 18, 2013, http://www.reuters.com/article/2013/01/18/us-china-

[2] Kevin Yao and Aileen Wang, "China's economy posts slowest growth since 1999," Reuters, January 18, 2013, http://www.reuters.com/article/2013/01/18/us-china-economy-gdp-idUSBRE90H03020130118, accessed March 20, 2013.

[3] Keith Alexander, "Keynote Address," Cyber Security and American Power, American Enterprise Institute for Public Policy Research, Washington, DC, July 9, 2012.

Chinese hackers are surely responsible for a large piece of that and, to date, neither U.S. corporations nor the American government have given China sufficient reason to halt that activity. Unless incentivized to do so, cyber theft from China will surely persist as the CCP aims to ensure that the Chinese economy continues to grow.

An additional benefit for China to the theft of American IPR is that it allows Chinese companies to grow at the expense of their American counterparts, which not only suffer the immediate effects of thefts, but must also must invest their limited resources to repair networks and protect against future incursions. Again, thus far, Chinese authorities have seen little need to halt an activity that may actually make American companies less competitive.

While ensuring the Chinese people continue to grow wealthier is itself a primary goal of the CCP, China's continued rise is also crucial if the party is to validate its claim that it and it alone can lead the country back to greatness. The CCP has long propagated a victim narrative of Chinese history, and nationalist education has been particularly emphasized since the aftermath of the Tiananmen Square massacre. In that narrative, China was Asia's central power, or "Middle Kingdom," for millennia before Western powers brought it down and inflicted upon it a so-called "century of humiliation." It is the CCP who can right those wrongs and return China to its rightful place atop the Asian hierarchy.

To do so, Beijing must restore sovereignty over territories wrongfully taken from it, including Taiwan and disputed islands in the East and South China seas. Doing so would not only allow Beijing to complete what it sees as a historic mission, but to enhance its own security. Controlling these islands and the surrounding waters would grant China greater strategic depth, allow it to more easily safeguard or control sea lines, and permit it to more easily access the Pacific and Indian oceans. Of course, these waters are also home to U.S. treaty allies (South Korea, Japan, the Philippines, Thailand, and Australia further afield), long-standing security partners (Taiwan and Singapore), and new friends (Indonesia, for example). It is in these littoral regions where tensions have been running high, where conflict is most likely to break out, and where U.S. and Chinese interests directly clash.

For China, cyber capabilities are tools to be used in pursuit of its own interests in this region. In particular, China likely uses or will use cyber capabilities for three related, but different, purposes. First, Chinese hackers will engage in espionage activities in the pursuit of both strategic and tactical intelligence. This, of course, is a natural activity in a competitive relationship—the United States and China are going to spy on one another. The question is, what new counter-intelligence tools are needed to meet this relatively new espionage threat? The more traditional tools of espionage are inherently risky—intelligence operatives can be arrested, spy planes can be shot down—but the risks to hacker-spies are not so clear. How can the United States make cyber espionage a riskier proposition for China and others?

Second, the People's Liberation Army (PLA) will use cyber warfare as part of its suite of anti-access/area denial (A2/AD) capabilities. The PLA has been developing systems aimed at keeping U.S. forces distant from Chinese shores, complicating in particular the U.S. Navy's ability to operate freely in the Asia-Pacific theater and thus making U.S. intervention in a Taiwan Strait or other conflict more difficult. Much of the attention to China's A2/AD capabilities has rightly focused on its missile forces, naval capabilities, and air defense systems. But cyber capabilities play a role in A2/AD, as the Defense Department's 2012 report on Chinese military power made clear:

> China's leaders in 2011 sustained investment in advanced cruise missiles, short and medium range conventional ballistic missiles, anti-ship ballistic missiles, counterspace weapons, and military cyberspace capabilities which appear designed to enable anti-access/area-denial (A2/AD) missions, or what PLA strategists refer to as "counter intervention operations."[4]

In the event of a conflict, PLA cyber forces will likely aim to disrupt U.S. military command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks. These efforts will complement attacks with more conventional, "kinetic" weapons to essentially blind, deafen, and silence U.S. forces. It should be noted that the 2012 DoD report on China's military included "cyber weapons" among the PLA's "counterspace capabilities" as well.[5]

As with Chinese cyber espionage, these developments are concerning, but they shouldn't be surprising. It is not unnatural for China to adopt military measures aimed at countering U.S. military advantages—in particular, advanced C4ISR capabilities—which also happen to represent critical vulnerabilities. For U.S. military planners, the questions are clear, though the answers may not be. How can the American military enhance defense against cyber attack? Does the PLA have vulnerabilities of its own that are susceptible to cyber warfare? What vulnerabilities do China's cyber forces themselves have to counter-attack, whether cyber or kinetic? Is it possible to take China's cyber forces out of the fight early in a conflict?

More worrying than China's theft of intellectual property, its espionage activities, or its development of cyber weapons for use at the tactical and operational levels, however, is China's development of strategic cyber weapons. Recent revelations of Chinese cyber intrusions into U.S. critical infrastructure are especially troubling. No government can easily tolerate a state of affairs in which its country's electrical grid, water supply, financial stability, or transportation security are held at risk by an anonymous hacker half a world away.

---

[4] "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012," Department of Defense, May 2012, p. iv
[5] Ibid., p. 9

Yet even worse is that China's development of these capabilities is potentially destabilizing. Because these weapons lack the ugliness of nuclear weapons—there is no radiation and they don't immediately and directly cause widespread death and destruction—not to mention the fact that their origin may be difficult to trace, Beijing may come to see them as more "useable" than nuclear weapons. And with such weapons likely to be seen as adding an intermediate step on the escalation ladder—one preceding the use of nuclear weapons—Beijing may come to see armed conflict as less dangerous than it otherwise would have. Conflict would become even more likely if Beijing believes that the American response to a strategic cyber attack would be one that China can tolerate.

Ideally for China, of course, its possession of such capabilities would ensure it never has to use them. Cyber weapons for A2/AD would keep U.S. forces physically distant from a fight in China's neighborhood, while Chinese strategic cyber weapons would deter the United States from attempting to expand or otherwise escalate the conflict. Meanwhile, effective espionage would allow China to more accurately predict U.S. actions, to gauge U.S. vulnerabilities, and to speed along its own military modernization. At the same time, theft of IP and trade secrets would be making American companies less competitive, putting a drag on the U.S. economy and putting further budgetary pressures on defense spending.

American Policy Options

I knowingly paint a dire picture here, but it is thankfully one that need not be borne out. There are steps the United States can take to arrest China's use of cyber capabilities and ensure American national security going forward. The suggestions below, all of which require further thought, fall into three broad categories: legal, diplomacy, and military.

In a recent article for *Foreign Policy*, Dan Blumenthal, director of Asian Studies at the American Enterprise Institute, applauds the Justice Department for tackling the issue directly through its formation of the National Security Cyber Specialists' Network (NSCS), which is exploring the potential prosecution of cyber criminals and whether that would have a deterrent effect on other hackers. But Blumenthal argues that new legislation is required:

> …Congress could also consider passing laws forbidding individuals and entities from doing business in the United States if there is clear evidence of involvement in cyber attacks.
>
> Congress could also create a cyberattack exception to the Foreign Sovereign Immunities Act, which currently precludes civil suits against a foreign government or entity acting on its behalf in the cyber-realm. There is precedent: In the case of terrorism, Congress enacted an exception to

immunity for states and their agents that sponsor terrorism, allowing individuals to sue them.[6]

Blumenthal also cites a paper by Jeremy A. Rabkin and Ariel Rabkin, in which the authors propose that Congress use its constitutional power to grant "letters of marque" to privateers. The idea would be to essentially coopt American hackers—effectively granting them immunity and perhaps funding if they agree to target only those countries or entities approved by Congress. This would allow for less provocative but still semi-official retaliation for attacks on U.S. entities.[7]

Diplomatically, there are several paths to pursue. The Obama administration's recent willingness to repeatedly raise the issue of Chinese cyber incursions, both publicly and privately, is a good first step, which will begin to convey to Beijing how seriously the United States is taking the matter. Ideally, China will be willing to join in a broad-based international effort to establish norms and rules of the road in the cyber realm. But China will need incentive to do so, and at present its experience in the current world of cyber is one of much gain and little pain.

The Obama administration, then, must begin to match its words with actions. In a recent speech to the Asia Society, National Security Advisor Tom Donilon asserted that cyber threats pose risks "to international trade, to the reputation of Chinese industry and to our overall relations." It is time for the administration to begin elucidating just what those risks are. Potential steps could include limiting the access to the U.S. market for Chinese state-owned enterprises and for any Chinese companies determined to have benefited from theft of American trade secrets. The administration could also consider the feasibility of filing suit at the WTO.

The administration can also work with allies and partners to encourage more responsible behavior in cyberspace. For example, like-minded countries could establish a preferential trade agreement, which would require strict adherence to a set of cyber crime legal standards for membership. Alternatively, victims of cyber theft and cyber attacks could establish a shared set of punishments, such as those listed above, that they agree to impose.

In the military sphere, the United States should be clear about how it will respond to the use of strategic cyber weapons on American soil. Beijing should not be confident it can carry out an "untraceable" cyber attack and should have a clear understanding of the consequences in the event of attacks against U.S. critical infrastructure. The

---

[6] Dan Blumenthal, "How to Win a Cyberwar with China," ForeignPolicy.com, February 28, 2013, http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china, accessed March 20, 2013.

[7] Ibid.; Jeremy A. Rabkin and Ariel Rabkin, "To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict," Hoover Institution, 2012, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf, accessed March 20, 2013.

Department of Defense should explore whether it is possible to conduct cyber exercises that will effectively demonstrate U.S. capabilities, much as conventional exercises are used, for example, to deter North Korea. In his *Foreign Policy* article, Blumenthal suggests that the "U.S. military could set up an allied public training exercise in which it conducted cyberattacks against a 'Country X' to disable its military infrastructure such as radars, satellites, and computer-based command-and-control systems."

But multilateral security efforts can go even further than exercises. Blumenthal argues that "the United States should set up a center for cyberdefense that would bring together the best minds from allied countries to develop countermeasures and conduct offensive activities." Not only would this allow for more effective development of advanced capabilities, but it would enhance deterrence as well. Chinese actions against one country could send all partners into action via the "cyber defense center," and an attack on the center would be an attack on all of the partner nations.

Cyber threats pose serious risks to the U.S. economy, the U.S. military, and American national security more broadly. China, in particular, is making use of cyber capabilities to pursue its interests at the expense of America's own. Working with allies and likeminded partners and, wherever possible, with China as well, the United States should be able to secure itself against these growing threats while hopefully establishing norms of behavior in cyberspace from which all nations can benefit.