This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

China's Growing Cyber War Capacities

https://www.e-ir.info/2012/07/29/chinas-growing-cyber-war-capacities/

MATTIA NELLES, JUL 29 2012

China's Growing Cyber War Capacities: A Threat to US Interests in Cyberspace?

With its continuous economic growth, soaring exports and growing military, China's rise and its implications for the existing super power the United States and more generally the world order is one of the predominant topics in strategic IR discourse. Issues like trade, monetary policy, intellectual property, military affairs or human rights on the other hand are the more prominent issues of the official bilateral US and Chinese policy agenda. However, in the age of the third industrial revolution,[1] both government and the private sector increasingly rely on digital assets for their production of goods and provision of services and as the digitalization and the reliance on such continue a very controversial issue appears also in the foreign policy debate: Cyber warfare and the threats of cyber attacks from foreign states, such as China. Given the growing Chinese cyber assets and cyber activity this essay asks whether and how the buildup constitutes a potential threat to US cyber interests and Sino-American relations. First, it is important to note that defining cyberwar or cyber threats is extremely difficult.

Before delving into analysis, this essay will briefly define how the term is used in this paper and elaborate on three distinct problems related to cyber war: the advantage of offensive strategies, the problem of attribution, and the problem of deterrence. Next, it will focus on two distinct forms of attacks: military and non-military attacks, particularly cyber espionage as opposed to the myriad other types of cyberattacks available to states and non-states. The second and main part of this essay is China's cyber foreign policy, analyzing and briefly evaluating China's military cyber assets. It will then raise the question of how those capabilities could be deployed in a hypothetical conflict with the US before examining the non-military cyber activities of China's cyber foreign policy, primarily cyber espionage. To assess China's cyberpower recent reports, this essay reviews analyses and some of the most prominent examples of what can be referred to as 'Sino cyber intrusions' (Hartcher 2010)

Cyberwar

The term cyber warfare is both ambiguous and controversial because there is no official or generally accepted definition. The increasing global dependence on information and communication technology poses risks not only for private users and businesses, but also for critical infrastructure, such as national energy systems, the financial sector, the aviation or transport sector, the health sector, and the government agencies (Adams 2001, 1). President Obama, the first US president to publicly discuss those specific cyber threats emphasized the importance of securing the nation's digital infrastructure in his May 2009 remarks, declaring it "a strategic national asset" (Nakashima and Krebs 2009). Consequently, an act of cyber aggression is understood as a targeted attempt to destroy or temporarily interrupt critical information infrastructures through cyber means. The attack on Estonia's digital infrastructure of 2008, the Stuxnet virus 2010 against the Iranian nuclear facilities or the latest attack against Iran's oil infrastructure on May 23 of this year are only three selected examples of those actions (Rid 2012).

Not only is it possible to attack and interrupt civilian infrastructure, but states or non-state actors can also utilize cyber-attacks as preludes to conventional military strikes. In 2003, Israel allegedly used cyber-attacks to obstruct Syrian air defense systems and in 2008, Russia used cyber-attacks against Georgian intelligence and other defense systems in the prelude to its land based invasion of South Ossetia (Rid 2012). In 2011, the Obama administration discussed the usage of cyber-attacks against the Libyan defense systems, however, Obama himself eventually

decided against it, fearing it might set a precedent for other nations—Russia or China in particular. (Schmitt and Shanker 2011).

It is important to note that these are the most extreme cases, and thus far rarer forms of cyber warfare.[2] More frequently, cyber means are used to infiltrate information systems to exploit, spy, or steal critical data. For the course of the paper I will primarily focus on the cyber-attacks by Chinese hackers that target US government or military institutions and security related businesses. Note that a distinction between state and non-state attacks is extremely difficult and most of the time the origin and motivation is based on official assessment rather than certain evidence. The theft of other private-sector and intellectual property like the famous AMSC case of 2011 remains a major bilateral issue between the US and China but will be excluded from the following analysis.

Given the broad working definition of cyber war, three more problems must be addressed: the advantage of attacks, and the problem of attribution and deterrence. Recently retired deputy Secretary of Defense Lynn in 2010 writing about the Pentagon's new cyberstrategy identified three problems of cyber warfare, which are crucial for the understanding of the Chinese motives, fleshed out in the second part. Lynn argues that due to the inherent open structure of the internet, the defender faces an asymmetric strategic challenge. Mounting attacks at this stage are always easier and cheaper than defending such attacks. Thus, technology today favors an offensive rather than defensive approach (Nye 2011, 125).

Unlike traditional warfare, the origins of sophisticated cyber-attacks are nearly impossible to trace. Determining where an attack originated is exceedingly difficult and by no means assured. This problem of attribution, as Lynn argues, has some real importance in that it begins to break down the paradigm of deterrence that was the undergirding of nuclear forces in the Cold War: "If you don't know who to attribute an attack to, you can't retaliate against that attack, so you can't deter through punishment, you can't deter by retaliating against the attack" (Lynn 2010, 1).

Some experts believe that China's growing military is aimed at deterring America from intervening in a future crisis over Taiwan. China, over the course of the last 20 years, invested heavily in "asymmetric capabilities" to counter America's once-overwhelming capacity to exercise power in the region. This "anti-access/area denial" approach includes "thousands of accurate land-based ballistic and cruise missiles, modern jets with anti-ship missiles, a fleet of submarines (both conventionally and nuclear-powered), long-range radars and surveillance satellites, and cyber and space weapons intended to 'blind' American forces" (The Economist 2012).

However, very little is known about the real number that China invests to pursue its "anti-access/area denial" approach. In the same way the effectiveness of its military cyber assets remain topic of a public, academic and security debate. So based on what is publicly known how strong is China's cyberpower? Two recent studies of national cyber power have placed China near the bottom of the table. On the EUI-Booz Allen Hamilton Cyber Power Index China is ranked 13th after Argentina, Mexico, and Brazil but better off than Russia, Turkey, South Africa, and India. Interestingly, the United Kingdom, United States, and Australia are the top three (The Cyber Hub, 2012). The second ranking on cyber security or cyber defense was made by the Brussels-based Security and Defense Agenda, which places China with Italy, Russia, and Poland in the fifth tier (the U.S. and the U.K. are in the third tier, below Finland, Sweden, and Israel and the top group is empty) (Miks 2012). Adam Segal, Senior Fellow at the Council on Foreign Relations, reviewing these two studies concludes that both mentioned studies are very subjective as they are based on interviews, surveys, and vague metrics (Segal 2012). Moreover, he questions the coherence and efficacy of Chinese cyber (defense) strategy. Given the ambiguity in China's offensive as well as defensive capabilities, it is worth looking first at the militarized components of its cyberpower and then on the more frequent and currently controversially discussed part of its cyber activity, the cyber espionage.

China's Military Cyber Assets

Bearing in mind the reports on China's cyber power and cyber defense capability the assessment of China's militarized parts, explicitly not cyber espionage, is not as clear cut as its cyber espionage capability, to which I will turn in the next part. The basic question is how can the People's Liberation Army (PLA) or other branches of the

Chinese military use cyber means against US military or military related targets to potentially gain leverage in conflict scenarios.

Whereas it is true that China's investment into its military is rising constantly, only few scholars or experts see the US military cyber war capability lacking behind its Russian or Chinese counter parts. One of those few is Jeffrey Carr.[3] In a recent article, called 'Why US Will Lose a Cyber War,' he argued we currently witness a 'Rise of a Cybered Westphalian Age'. The basic argument is that due to the increasing reliance on technology in both the civil and military sectors vulnerability increases drastically. Given the described advantage of the offensive and the fact that countries with vastly growing economies like China that currently massively invest into offensive technology the outcome of a potential cyber war might already be determined:

"There's not another nation in the world that can wage kinetic warfare as effectively as the United States, and that's probably at the heart of the reason why the United States will lose a war fought in cyberspace" (Carr, 2010).

Whereas many experts share Carr's basic assumption about the increasing vulnerability, they disagree with the outcome he predicts. The basic questions are: How far developed are China's military equipment and how fast are these capabilities growing? How efficient could they be when used in combination with other military units?

More generally speaking it seems very unlikely that the world's military super power will be overwhelmed by the People's Liberation Army cyber war assets. To back up that claim, it is worth considering the most effective cyber war strikes, launched by militaries. Stuxnet, by far the most sophisticated cyber-attack on record, was most likely a U.S.-Israeli operation (Rid 2012). Another highly effective example of an effective military cyber-attack was used to blind the Syrian radar during the Israeli air strike on the Syrian nuclear facilities in 2007 (Markoff 2010). So, Rid concludes that "when it comes to military-grade offensive attacks, America and Israel seem to be well ahead of the curve" (Rid 2012).

Recently, the congressional US-China Economic Security Review Commission (USCC)[4] commissioned a report from Northrop Grumman on Chinese cyber war capacities and their possible strategic objectives. In the following part on espionage this report will be further examined. On the military side the Grumman report suggests, one possible scenario where the Chinese could effectively use their capacities is in a conflict over Taiwan. As only one example, the report notes that if the Chinese could redirect US air-refueling tankers away from where they are needed to refuel fighters and bombers, China could successfully delay a US attack (Shobert 2012). Another asset, even though more cybernetic than cyber, that could potentially weaken the military presence of the US in a potential strait conflict is China's growing UAV capabilities. The Washington based Jamestown Foundation recently reported that China's unmanned aerial vehicles could disrupt US aircraft navigation and possibly communication (Focus Taiwan 2012). To summarize, China's military cyber capability might be growing but it is expected that it cannot, at this stage, be effectively used in direct military clashes between the US and China to potentially overcome the great difference in size and efficiency of the US military.

China's Cyber Activity

Theft of intellectual property of has long been a concern of the US and other industrialized nations that invested in China. Considering the aforementioned problems of attribution, how do affected businesses know that the attackers are Chinese? Even if the attacks are launched from Chinese soil, what is the role of the Chinese government?

NPR cites Mandiant Beytlich, an intelligence officer, saying that Chinese hackers can't be identified by their IP address but solely by the way they work:

"They have quirks, maybe even the way that they type, the way that they select commands [and] the way that they build their software […] There's probably 20 or more characteristics you can use, none of which involve an IP address" (Gjelten, 2012).

Cartwright, former vice chairman of the Joint Chiefs and notable cyber expert, backs these claims and said that

Chinese cyber spies largely backed or directed by the government" are stealing key data. US officials have long complained about countries that systematically hack into U.S. computer networks to steal valuable data. Despite the technical problems with tracking back the attacks, American officials seem confident about the origin of the rising intrusions (The Associated Press, 2011; Gjelten, 2012).

In January, Lynn, Chertoff, and McConnell[5] published an op-ed called "China's Cyber Thievery Is National Policy-And Must Be Challenged". The authors, distinguished former public servants, asserted that "the Chinese are the world's most active and persistent practitioners of cyber espionage today" (Lynn; Chertoff; McConnell 2012). It is fair to counter that a lot of countries and criminal non-state actors nowadays embraced cyber espionage to gain a competitive edge. But it seems as if China stands out as especially aggressive.

A Northrop Grumman report, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," (a prelude of the already mentioned report from 2012) said that Beijing appeared to be conducting "a long-term, sophisticated, computer network exploitation campaign against the U.S. government and its military contractors" (Northrop Grumman 2009: 51). The follow-up report reiterated that trend and explicitly mentioned China and Russia as being the most active countries, engaged in cyber espionage (Northrop Grumman 2012). Over the recent past, official U.S. concern over alleged Chinese espionage has consistently grown. By some estimates the economic cost of the intrusions has risen to up to $400 billion worth of data each year (The Week 2012). Other than direct economic losses for US enterprises the national security is also affected by the theft. Some of hacked companies have contracts with the Defense Department and other U.S. government agencies, putting classified information at risk.

The editor of the Sydney Morning Herald tried to categorize the systematic intrusions with the following observation:

"In the first generation, they aimed at vital national security nerves – the Pentagon's networks, defense companies, resource firms and critical infrastructure. But the latest wave of Chinese intrusions into US computer networks is intended to steal intellectual property on a vast scale" (Hartcher 2010).

Empirical evidence seems to support the claim that Chinese cyber espionage is on the rise. Rogin writing for the Foreign Policy in 2010 stated that it is widely believed in US security circles that the Chinese government is supporting hackers that attack anything and everything in the U.S. national security infrastructure on a constant basis:

The Defense Department has said that the Chinese government, in addition to employing thousands of its own hackers, manages massive teams of experts from academia and industry in "cyber militias" that act in Chinese national interests with unclear amounts of support and direction from China's People's Liberation Army (PLA) (Rogin).

Moreover, Rogin lists the top 10 Chinese intrusions of which we are aware and a widespread attack on the State Department's East Asia Bureau is one of the examples. Attackers in 2006 breached the security system, breaking into information systems at U.S. embassies all over the region and eventually penetrating systems in Washington as well. Perhaps the most famous example is the major theft of tactical information from Lockheed Martin's F-35 fighter program, one of Americas most advanced airplanes. The multi-layered infiltration apparently went on for years without detection. The first reports in 2009 suspected Chinese hackers were behind the attacks. Reports in 2010 backed the claim (Rogin 2010).

Conclusion

As this paper argues, the military side of China's cyber foreign policy is still relatively underdeveloped. In scenarios facing superior maritime powers, such as the US, China's cyber assets could not give the country any advantage that could possibly bridge the gap in military strength. Regarding cyber activity, however, espionage plays a big role. Theft of intellectual property from private businesses and the intrusions of Chinese government and government related hacker groups pose a significant problem for US (cyber) interests. US officials and corporate leaders are

increasingly worried about the loss of expensive technology and the theft of military applications. More broadly speaking, this theft undermines the information-intensive U.S. economy. Fontaine concludes that “vast economic espionage, conducted largely through cyber operations, can diminish the United States’ strategic competitiveness” (Fontaine 2012).

Given the large problem of attribution, the difficulty of deterrence as well as the advantage of offensive attacks, in this case the infiltration of information systems to get the desired secret data, the asymmetric form of cyber warfare gives non-state actors and leaders in Beijing an incentive to pursue an aggressive cyber foreign policy. But there is a flip side to Beijing’s cyber offensive – what some call the ‘strategic costs’ it imposes on China itself. The basic argument is that the aggressive Sino cyber posture might spur backlashes in other policy fields and more generally the US-Sino relations. Arguably, the whole cyber issue could also have regional repercussions and potentially undermine China’s ‘smile diplomacy’ and its soft power initiatives to ease the fears of its neighbors about its rise.

While it is difficult to prove origin, the scale, organization, and intent of the attacks leads experts and officials alike in a lot of the recent cases to one sponsor in a lot of the recent cyber espionage: the Chinese government. So, even if the PLA or Beijing are not directly responsible for the increasing cyber espionage the international pressure on them is growing and the long-term political or strategic costs of its actions could soon exceed the short-term benefits.

Bibliography

Adams, James (2001): Virtual Defense. In *Foreign Affairs May/June* 80 (3). Available online at http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense, checked on 24 April 2012.

Focus Taiwan (2012): China’s UAVs capable of disrupting U.S. aircraft carriers: reports. Edited by Focus Taiwan News Channel. Available online at http://focustaiwan.tw/ShowNews/WebNews_Detail.aspx?Type=aIPL&ID=201206240013, checked on 24 April 2012.

Fontaine, Richard (2011): China’s Cyber Moves Hurting Beijing. Edited by The Diplomat. Available online at http://the-diplomat.com/2011/11/09/china%E2%80%99s-cyber-moves-hurt-beijing/, checked on 24 April 2012.

Gjelten, Tom (2002): U.S. Not Afraid To Say It: China’s The Cyber Bad Guy. Edited by NPR. Available online at http://www.npr.org/2012/02/18/147077148/chinas-hacking-of-u-s-remains-a-top-concern, checked on 24 April 2012.

Hartcher, Peter (2010): Cyber attacks take aim at the heart of the American empire. Edited by Sydney Morning Herald. Available online at http://www.smh.com.au/opinion/politics/cyber-attacks-take-aim-at-the-heart-of-the-american-empire-20100201-n8s0.html, checked on 24 April 2012.

Letch, Simon (2010): Picture used in Hartcher.

Lynn, William J. (2010): Defending a New Domain. The Pentagon’s Cyberstrategy. In *Foreign Affairs May/June* 89 (5). Available online at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, checked on 24 April 2012.

Markoff, John (2010): A Silent Attack, but Not a Subtle One. Edited by New York Times. Available online at http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=1&hp, checked on 24 April 2012.

McConnell, Mike; Chertoff, Michael; Lynn, William J. (2012): China’s Cyber Thievery Is National Policy—And Must Be Challenged. Edited by Wallstreet Journal. Available online at http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html, checked on 24 April 2012.

Miks, Jason (2012): Israel, China and Cyber Security. Edited by The Diplomat. Available online at http://the-diplomat.com/the-editor/2012/02/02/israel-china-and-cyber-security/, checked on 24 April 2012.

Nakashima, Ellen; Krebs, Brian (2009): Obama Says He Will Name National Cybersecurity Adviser. Edited by Washington Post. Available online at http://www.washingtonpost.com/wp-dyn/content/article/2009/05/29/AR2009052900350.html, checked on 24 April 012.

Northrop Grumman (October 2009): Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. Edited by USCC. Available online at http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf, checked on 24 April 2012.

Northrop Grumman (2012): Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Edited by USCC. Available online at <http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2012/03/08/National-Security/Graphics/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf>, checked on 24 April 2012.

Nye, Joseph S. (2011): The future of power. New York: PublicAffairs.

Rid, Thomas (2012): Think Again: Cyberwar. Edited by Foreign Policy Magazine. Available online at http://www.foreignpolicy.com/articles/2012/02/27/cyberwar, checked on 24 April 2012.

Riley, Michael A.; Vance, Ashlee (2012): China Corporate Espionage Boom Knocks Wind Out of U.S. Companies. Edited by Bloomberg. Available online at http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html, checked on 24 April 2012.

Rogin, Josh (2010): The top 10 Chinese cyber attacks (that we know of). Edited by Foreign Policy Magazine. Available online at http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of, checked on 24 April 2012.

Schmitt, Eric; Shanker, Thom (2011): U.S. Debated Cyberwarfare in Attack Plan on Libya. Edited by New York Times. Available online at http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html, checked on 24 April 2012.

Segal, Adams (2012): Is China a Cyber Paper Tiger? Edited by The Diplomat. Available online at http://the-diplomat.com/flashpoints-blog/2012/02/09/is-china-a-cyber-paper-tiger/, checked on 24 April 2012.

Shobert, Benjamin: China's capacity for cyber-war. Available online at http://www.atimes.com/atimes/China/NC15Ad01.html, checked on 24 April 2012.

The Associated Press (2011): Chinese cyberspies stealing key data, U.S. analysts say. Available online at http://www.cbc.ca/news/technology/story/2011/12/12/china-hackers-us.html. Checked on 24 April 2012.

The Cyber Hub (2012): The Cyber Power Index. Available online at http://www.cyberhub.com/CyberPowerIndex. Checked on 24 April 2012.

The Economist (2012): China's military rise. Edited by The Economist. Available online at http://www.economist.com/node/21552212. Checked on 24 April 2012.

[1] For a more refined definition of the third industrial revolution and what the reliance on digitalization means for the chain of production and the creation of services see the Apr 21st, 2012 edition of the Economist.

[2] For a more refined definition of cyber war and its various forms see Joseph Nye's chapter on 'cyberpower' in his recent book ‚The Future of Power' (2011).

[3] Jeffrey Carr is the founder and CEO of Taia Global, Inc. and the author of "Inside Cyber Warfare". He regularly

consults with Global 2000 corporations and agencies of the U.S. and allied governments on Russian and Chinese cyber warfare strategy and tactics as well as new and emerging threats.

[4] The USCC is a 12-member bipartisan commission set up by Congress in 2000. The body investigates national-security implications of U.S. trade with China.

[5] McConnell is a former director of national intelligence and before that he served as the director of the National Security Agency. Chertoff served as secretary of homeland security.

—-

Written by: Mattia Nelles
Written at: The University of California, Berkeley
Written for: Professor Hon Yung Lee
Date Written: April 26, 2012