U.S. China Security and Economic Review Commission
"China's Information Controls, Global Media Influence, and Cyber Warfare Strategy"
James A. Lewis, Center for Strategic and International Studies
May 4, 2017

China finds itself in a remarkably fortunate position. The United States, its chief strategic competitor, has been weakened by intractable wars in the Middle East and political turmoil at home. Russia, which could be a strategic competitor, has chosen instead to partner with China against the U.S., and in any case, is in decline as a great power. No other country in the region or outside poses a significant challenge to China.

It would be an overstatement to say that Xi Jinping inherited a crisis, but the trends for China and, more importantly, for continued Party rule, were not positive when he arrived. China faces serious political, economic and environmental problems, but the Xi government has worked energetically to reduce political risk. Xi's efforts to reduce corruption, centralize intelligence tasking, and reform and modernize the PLA have the added benefit of reinforcing Xi's authority.

Controlling the internet and information play an important part in this effort. China's information policy has four goals. They are to reduce risks to political stability and continued Party rule; promote Chinese content and technology; reshape global rules to favor China's interests; and defend against perceived U.S. hegemony. China, in the last few years, has created policies, regulations and to make the information environment in China more controllable, most recently with the "National Cyberspace Security Strategy" released late last year.

China, along with Russia, promotes a reassertion of national sovereignty. This reflects in part an erosion of western and American influence and in part recovery from the collapse of communism. We could call this reassertion the "authoritarian alternative," an effort to replace the U.S.-led international order and to rebalance the relationship between sovereignty and "universal" values. Russia and China reject the idea of universal values, saying these are in fact 'western values" that are inappropriate for non-western nations. This line of reasoning has some appeal with some non-aligned nations, and China has benefited from the Russian campaign to exploit the Snowden leaks and other purloined materials to attack the idea of democratic institutions and universal values.

Before 1945, sovereignty was absolute within a nation's borders. Non-interference in internal affairs was the norm for state behavior. Since 1945, the predominant view is that there are issues, such as human rights, that transcend borders. The UN Charter, the Universal Declaration of Human Rights, and the agreements establishing the World Trade Organization, are all examples where nations including China, have voluntarily surrendered some of their sovereign authorities. Fundamentally, Russia, China and other authoritarian regimes seek to reclaim sovereign authority. The goal is to give national sovereignty greater influence, legitimizing government control of national networks, and to restore older concepts of inviolable sovereignty.

In the last few years, China has articulated a new and coherent view of cyberspace that places sovereign control at the center of national and international policy. China's new National Cyberspace Security Strategy assert that "National sovereignty extends to cyberspace, and

cyberspace sovereignty has become an important part of national sovereignty." The concept of cyber sovereignty is part of this reassertion. President Xi defined the elements of cyber sovereignty at the 2016 Wuzhen conference as "respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace—avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries."[1] China's views on sovereignty seeks to reassert the dominant role of states within the context of an approach to globalization that seeks to amend rules, institutions and, standards in ways favorable to its own interests and more consistent with its own political views.

This vision has been accompanied by a substantial reorganization of the State and Party apparatus for dealing with cyberspace, including the creation in 2014 of a Central Leading Group for Internet Security and Informatization, chaired by President Xi, and a new Agency, the Cyberspace Administration of China (CAC). Other actions to reinforce domestic control include restrictions on Virtual Private Networks and disruptions to the service they offer, and new limits on social media by deleting posts and closing accounts. The Leading Group sets policy and the CAC implements, improving China's control over domestic networks and internet users. These changes are the result of a deep interest by President Xi in extending control over cyberspace, which he has identified (along with corruption) as a key threat to political stability and continued party rule.

China has been successful in extending sovereign control to the internet. As the internet is based on physical infrastructure located within national territory, it is easy to control many functions. Beijing blocks access to and traffic from foreign sites of which it does not approve. This does not come without economic costs, as Chinese researchers and businesses cannot access useful information and services, but this is a price that Beijing is willing to accept. China the only country to impose national control over the internet and other countries are moving toward greater localization of data and apply national laws to the internet. The is not the borderless one-world that American technologists so confidently expected, but neither is it the dreaded "fragmentation" of the internet. What is interesting is that while many countries are asserting control over the internet, here is very little effort in China or elsewhere to coordinate or multilateralize these controls, reflecting widely disparate views on privacy and the treatment of data.

The impetus for greater control and reducing risk motivates a parallel effort at industrial policy. China's motives in expanding its information technology sector are both commercial and political. Since the 1980s, China has sought to build a strong information industry and we have seen repeated efforts, such as the push for indigenous innovation, to achieve this. China has not hesitated to extract concessions or block foreign competition in the IT sector in pursuit of this goal. China employs various strategies to displace western companies, using non-tariff barriers, security regulations, procurement mandates, the acquisition (both licit and illicit) of foreign technology, and through strategic investments and the acquisition of western firms.

China is driven by the same supply chain security concerns heard in the U.S. and there is a long-standing belief in China that western technology is inherently untrustworthy. It is troubling that

[1] http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

this most likely reflects China's own intentions rather than the actual behavior of western companies. China legitimate desire for economic development is complicated by powerful commercial motives to use national investment produce globally dominant national champions in many different industry sectors.

The Chinese are aware of these limitations and have developed a new approach: to buy western companies rather than create a Chinese counterpart (China uses a similar strategy in its latest effort to create a domestic semiconductor industry, with a well-financed strategy to create a domestic industry intended to displace foreign suppliers). Creating a counterpart company and blocking western services (such as Weibo instead of Twitter) was an effective policy for controlling social media use by a domestic audience, but it is not effective overseas. It is too early to assess the effect of China's media purchases, [2] but when Alibaba bought the South China Morning Post it was with the explicit goal of creating more positive coverage of China.[3]

China's informational campaign seeks to use western media formats to shape foreign views of both China and the U.S. in ways favorable to it (Russia uses RT in a similar fashion). The Global Times, the effort by Peoples Daily to cooperate in shaping overseas opinion, is only slightly more persuasive than RT. It is more likely that the Chinese government will encourage new owners to ensure that favorable views of China are presented in films or the media - a kind of soft propaganda - rather than to win support for specific Chinese positions.

Russia has used its long experience, dating back to the Czars, in what we would now call information operations. These operations to produce cognitive effect and shape the thinking of opponents and neutrals are a central element of Russian military doctrine and what Russia calls "New Generation Warfare." In contrast, the Chinese do not have similar military doctrine on opinion shaping.

China's own information operations suffer from a lack of subtlety and attractiveness. Chinese propaganda is effective in shaping the views of a domestic Chinese audience, but has far less traction in other countries. While these information operations are very effective in influencing the views of a Chinese audience, they are much less successful in other cultural and linguistic arenas. The opportunity to play the role of supernumerary in the "China Dream" does not attract many adherents.

China and International Cooperation in Cybersecurity

Multilateralizing China's online restrictions plays a tertiary part in this effort. China's primary focus is domestic. It's primary negotiating goal is to avoid agreements that could increase political or military risk - Chinese interlocutors have expressed concern, for example, that a specific reference to the inherent right of self-defense[4] could legitimatize U.S. cyber actions against China. Promoting Chinese view on sovereignty, internet governance, or cyberwar come

[2] China and Russia may wish to recall the words of Lu Xun: "Lies written in ink can never disguise facts written in blood"

[3] According to Alibaba's vice Chair.https://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html?_r=0

4 Article 51 of the UN Charter

second to these domestic goals.

China has found a willing partner in Russia for its international efforts, but this is a marriage of convenience, not love. The Russians distrust the Chinese and the Chinese do not hold the Russians in high esteem. But both are united in this uneasy partnership by their desire to push back against the U.S. and the international order it created. They seek multilateral assent to norms that reduce the chances of events similar to the "Arab Spring" in their countries, to what they see as internet-inspired domestic unrest, something that both China and Russia fear.[5] Chinese interlocutors say that Social media and "Color Revolutions" are a threat, but that the party is in the process of learning how to deal with and use them for its own purposes, such as by using government employees (the Chinese equivalent of Russian media trolls) to plant millions of positive messages about the party and Chinese policies on social media sites[6].

China has a consistent approach to multilateral cybersecurity negotiations, to promote sovereign control and to safeguard its security and commercial interests. China's new National Cyberspace Security Strategy talks about "increasingly fierce competition" to "seize the right to develop rules." China has increased its involvement in international standards-making (previously the domain of western companies) for information technology both to garner commercial advantage and to revise standards, protocols, and architectures to improve government ability to control cyberspace. China is as yet unskilled in wielding its new power and influence, and while it is adept in pursuing its economic interests overseas, it is less effective in advancing its political agenda.

These multilateral activities include the Shanghai Cooperation Organization (SCO), discussions among "BRIC nations," efforts to promote their "International Code of Conduct for Information Security, and Chinese positions in the negotiations in the UN Group of Government Experts on information security (GGE). China has also tried to use its first World Internet Conference in 2014 to gain support for its ideas of "cyber sovereignty" and a multilateral approach to internet governance. (which would give governments a dominant role, in contrast to the current multi-stakeholder model). In each of these efforts, however, Russia and China have met with only mixed success. On internet governance, the Chinese appear to have accepted the IANA transition, where the U.S. government ended its contractual relationship with ICANN, as a legitimate change in internet governance that had made the issue less salient. This may also reflect greater Chinese confidence in their ability to manage the internet, to extend sovereign control over their own networks, and to reduce political risk.

Russia and China introduced their Code of Conduct[7] to challenge the international status quo and shift the terms of the global debate over cybersecurity and online freedoms in their favor. The Code essentially redrafts international commitments to increase the rights of the state vis-à-vis the rights of citizens. The chief problem with the Code is that many of its provisions are

[5] Chinese commentators expressed a degree of schadenfreude over the news of Russian interference in the U.S. elections. There sense was that the Russians had only done to the U.S. what the U.S. had been doing for years to governments it opposes.

[6] https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?utm_term=.9d718382c7fd

[7] https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

obviously intended to redefine and limit other international commitments, and in particular the Universal Declaration of Human Rights. Most Western observers believe it is an effort to amend international agreements in ways that strengthen sovereign authority at the expense of existing international commitments. Russia and China revised the Code in 2014 to soften these provisions, but even with these changes, it has attracted only limited support. U.S. opposition to the Code has been unwavering.

Similarly, the SCO has not met expectations for global influence. SCO is the poor man's NATO. It lacks the deep cultural affinity and shared historical experience that shapes the transatlantic alliance. While it reached agreement in 2009 on information security, its one major achievement has been to provide a multilateral veneer to the Code of Conduct. SCO has held one cybersecurity exercise, in 2015, focused not on a defense of critical infrastructure but on preventing Arab Springs by coordinating the removal of "terrorist" content on websites and social media.[8] This is a very different approach to cybersecurity, inward looking and focused on stifling dissenting views.

While Russia and China signed a cybersecurity pact in 2015, this was done largely for show, with intention of annoying the Americans. The pact was a Russian diplomatic maneuver to which China acceded. Some call it a "nonaggression pact," which should give the Russian pause, and to date there is no evidence of tangible cooperation between the two nations on cybersecurity.

Russia and China have made efforts to use the BRIC nations as a multilateral counterweight to the western alliance, with various initiatives, funds, and agreements that are announced at every BRIC meeting. These are also largely for show and noticeable for absence of any meaningful commitment of resources. The idea of the BRICs as a political alliance faces fundamental problems. It is worth bearing in mind that the term "BRICS" was coined by a business consultancy to describe economic trends and it suggests a certain poverty of imagination that Russia and China have embraced it as a political vehicle. To the extent the BRIC's share a goal, is it discontent with the current order of international relations rather than any deep cultural affinity or shared values, but China has so far been unable to capitalize on this diffuse discontent.

Attitudes towards fundamental rights create an immediate challenge for cooperation among the BRICs. India and Brazil are democracies with a strong commitment to free speech. However much they distrust the U.S., they are unlikely to abandon this commitment. Nor are China and India likely to forge a strategic partnership. If anything, they are strategic competitors. In simple terms, while India and Brazil may enjoy playing Russia and China against the U.S. and its allies, they are not going to move into the authoritarian camp. The NetMundial Conference, organized by Brazil in response the Snowden revelation of U.S. surveillance, ended by producing a powerful endorsement of democratic freedoms online that only Russia, Cuba and India opposed (somewhat sourly) and in retrospect, Indian officials say that they regret this opposition.

[8] First network anti-terrorism exercise successfully held in Xiamen, Xinhua, October 2015, Peter Wood, http://news.mod.gov.cn/action/2015-10/14/content_4624236.htm; Peter Wood, China Conducts Anti-Terror Cyber Operations With SCO Partners, Jamestown, October 2015, https://jamestown.org/program/china-conducts-anti-terror-cyber-operations-with-sco-partners/

This is a somewhat threadbare tapestry of diplomatic accomplishment in international agreement in cybersecurity, orchestrated by Russia and tolerated by the Chinese, with little tangible effect other than to create concern among gullible western observers and impose obstacles to any agreement on western terms. However important these maneuvers are to Russia in its effort to restore its international position, they are of secondary importance to China. The authoritarian alternative is simply not that attractive for most people. China's rulers, however, do not care. There is still a degree of insularity in China's views, reinforced by the belief that its vast population and growing wealth allow it to set its own course.

Cybersecurity Negotiations

Chinese (and Russian) views on international negotiations on cybersecurity are shaped by defensive requirements, to protect themselves from what they see as a hostile and technologically superior U.S. whose actions are largely untrammeled by international law and are motivated by plans to disrupt Chinese (and Russian) society and replace the current regimes with ones more in its own image. China, if anything, takes a more intransigent position that Russia in international cybersecurity negotiations. This may in part reflect the greater confidence Russia has in being able to control these negotiations, given its long history and experience in arms control. The Russians are the masters of this game and the Chinese, while increasingly skilled, remain more cautious and less flexible.

The focal point for international cybersecurity negotiations are the meetings of the UN GGE. The Report of the 2013 GGE reshaped the international discussion of cybersecurity. It recognized the requirement for nations to observe their international commitments in cyberspace, including the centrality and applicability of the UN Charter, International Law (including both International Humanitarian Law and the Universal Declaration of Human Rights), and national sovereignty. This report, later endorsed by the General Assembly embedded state practices in cyberspace in the existing framework of international relations and law. The 2013 Report and the consequent 2015 Report also identified a set of initial norms and CBMs, also endorsed by the General Assembly.

China was the nation that most strongly opposed these commitments, particularly to the applicability of international law, and by the end of the negotiations, it was the only nation that opposed them. It is likely that China finally agreed only because Presidents Xi and Obama were to meet at Sunnylands the day following the GGE's conclusion, and the Chinese did not want to place their leader in the position of explaining why China was the only country to oppose international agreement on cybersecurity. While China has grudgingly accepted the applicability of international law, it continues to show ambivalence over the treatment of cyber warfare, and it supports Russian proposals that existing international law is insufficient for cyber conflict and must be amended and expanded.

China promotes a very different vison of international order that reasserts the primacy of national sovereignty and devalues international agreements that constrain sovereignty, particularly the Universal Declaration of Human Rights. China is not alone in this and receive significant support from some nonaligned nations, notably Pakistan, Egypt and Malaysia, and from Russia.

China pursues international agreements that would reduce political risk and move in the direction of more traditional views of national sovereignty (increasing governmental authority over the internet. At the same time, it takes a defensive position in the international discussion of cybersecurity norms., seeking to block agreement on norms that could potentially be used to justify action against China for its cyber activities, such as a norm reinforcing the right to use Counter-Measures (e.g. retaliatory action that do not involve the use of force, such as sanctions or indictments).

China, along with Russia and some Non-Aligned Movement nations have called for a ban on cyberattacks and cyber "weapons." China has said that cyberspace should be a "zone of peace," while western nations say that we should recognize the widespread adoption of cyberattack for military purposes (including by Russia and China) and that its use should be regulated by international humanitarian law, as is the case with other military activities. These fundamental disputes over the extent to which sovereignty applies and the legitimacy of cyberwar shape international discussion of norms Chinese negotiating positions on cyber war reflect more than anything else the disconnect between the positions China's Foreign Ministry takes in international negotiations and China's actual military policies – the most salient example being the Foreign Ministry' steadfast calls for the demilitarization of space that continued until the day after China's 2009 ASAT test. The Chinese do not find it anomalous to call for banning weapons in cyberspace at the same time they actively pursue the development of such weapons and plan for their use.

Cyber Operations

Chinese negotiating positions do not reflect the actual capabilities of the PLA, which the Chinese believe are still significantly inferior to those of the U.S. Those familiar with China will not be surprised to learn that there is something of a disconnect between the military and foreign policy establishments. Paradoxically, PLA modernization and the public admission that China has something similar to the U.S. Cyber Command could make it easier to hold bilateral military talks with the Chinese.

"Winning informationized local wars" has been a theme in Chinese strategy for years. Recent organizational changes make this a more achievable goal, but in the long term. China's 2015 Military White Paper acknowledged China's plans to build capabilities for offensive cyber operations and to organize them in the new Strategic Support Force. The White Paper identified outer space and cyberspace as the "new commanding heights in strategic competition."[9] Chinese interlocutors do not see cyber as a weapon of mass destruction. Chinese military doctrine for cyber operations appears to be scenario based and limited, although some PLA representatives say this may changes when the Strategic Support force reorganization is complete in 2018 and develop broad doctrine and strategy (noting that it took the U.S. years after the creation of Cyber Command to develop doctrine for offensive cyber operations).

The most interesting thing about Chinese planning for cyber operations is that it seems to be specific to a few scenarios, part of a larger package of weapons and attacks intended to defeat

[9] China's Military Strategy: The State Council Information Office of the People's Republic of China, May 2015, Beijing, http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm

American carrier battle groups in the South China Seas and the Sea of Japan. Cyberattacks would be combined with electronic warfare, high-speed anti-ship missile strikes, and anti-satellite activities to defeat deployed U.S. forces. Chinese planning and doctrine for cyber operations do not appear to have the general applicability found in U.S. cyber doctrine and planning. This may reflect limitations in Chinese current military planning and organization, or China's larger strategic orientation, and this could change as the new Strategic Support Force matures. We may be guilty of "mirror-imaging" when it comes to explain Chinese planning for cyber operations, attributing to it strategic and global considerations similar to those that guide that guide U.S. thinking but not necessarily China's.

These differences in doctrine, strategy and capability, create a divide in Chinese and American views of cybersecurity that complicate negotiating efforts but also helps us to identify where agreement may be possible and where it is not. China's primary concern is internet content and its domestic political effect. America's primary concern has been espionage and the risk of attack on its domestic critical infrastructure, something that does not appear to be a central part of Chinese planning for cyber operations (nor is there any indication that China has mounted a campaign to subject the U.S. to a "death by 1,000 hacks").

This means that the space for agreement will be found in a discussion of international security that take into account China's fears about domestic political stability. The U.S. has some leverage in discussing cybersecurity with the Chinese. The Chinese fear Cyber Command; this means they will discuss restraints on cyber war. Some Chinese worry that a "techno-nationalist" approach to information technology will create economic damage, and China worries about its own vulnerabilities to hacking and cybercrime.

China and the U.S. will never approach human rights in the same way, but while there will be constant sparring over freedom of expression in any negotiation, and while it is essential to hold China accountable to the international community for its UN commitments to protect human rights, the areas of potential agreement involve avoiding miscalculation and misunderstanding in military operations, limits on espionage, and cooperation in cybercrime, subjects where both sides share common interest in avoiding miscalculation, controlling the potential for escalation, and cooperating to prosecute actions in cyberspace that are illegal in both countries.

In private, PLA representatives accept the U.S. ability to accurately authenticate the source of an attack. This does not yet appear to have greatly affected PLA planning for cyber operations. In the event of conflict, both sides intend to attack each other's command and control networks, weapons systems and reconnaissance assets. This is unavoidable, nor is it in the U.S. interest to agree to constraints that we would observe and others would not, or that do not fit with state practice in conflict. There would be benefit, however, from establishing formal mil-to-mil exchanges on cyber operations, the adoption of bilateral and regional confidence building measures, and the creation of mechanisms to reduce the chances of miscalculation or misinterpretation.

The Chinese say they are open to improved communication to manage the risk of cyber conflict and to increase stability. One obstacle is that the Chinese do not always seem confident of their own cyber capabilities when compared to the U.S., making them hesitant to pursue formal

discussion. They believe that the disparity between U.S. and Chinese military cyber capabilities is so great that it could be awkward for them to meet. One pre-condition for expand mil-to-mil discussion may be the need to wait for PLA reform to complete, but it may be possible in the next few years to have serious discussions of cyber operations through flag-rank exchanges, conferences, and other vehicles. The U.S. would need to carefully consider in pursuing bilateral exchanges the risk that it could unintentionally instruct China in how better to organize and plan military cyber operations.

Espionage is no longer the most salient topic. China appears to be living up to its commitments under the Obama-Xi agreement. The language of this agreement was carefully crafted by the U.S. to allow both sides to continue to engage in political-military espionage. It is not an agreement to end cyber espionage. China's reasons for agreeing to this owe as much to President's Xi's own agenda as to U.S. pressure. The agreement supports PLA modernization and reorganization by ending PLA units' cyber espionage moonlighting to augment their incomes. It advances Xi's goal of centralizing control of intelligence collection and assets under his control. The outcome of the agreement is likely to be a more effective and focused Chinese intelligence system, an unexpected consequence, but so far, Chinese commercial espionage against U.S. companies appears to have has decreased.

The Obama-Xi agreement showed that China's behavior and policy can still be influenced through engagement at senior levels, through realistic proposals, and with the threat, implicit or otherwise, of penalties, but it is far more difficult to do this than it was twenty years ago. U.S. policies need to adjust to a more assertive and independent China to identify where there is room for mutual understanding and where it will be necessary to build coalitions with like-minded nations to oppose further encroachments on universal values and the rule of law.

U.S. policy itself needs to be more assertive. Ultimately, the Chinese are pragmatic and will accommodate American concerns if persuaded it is best to do so. The West has a better hand to play (even if we do not always play it well), the Party's rule is fragile, and China's economy, despite its size, cannot grow without access to the West. A good first step, one where the U.S. might be able to persuade Europe to join us, is to insist on reciprocity in the treatment of foreign and Chinese companies. Reciprocity should be the catchphrase of China policy. The first step requires an honest assessment of how American views of the international relations will need to change from expectations in the 1990s of perpetual American predominance to fit a more world of greater conflict and competition.