Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia
James Lewis
Prepared for the Lowy Institute MacArthur Asia Security Project

Executive summary

Cyber infrastructure is critical to the global economy. Yet it is badly secured, worse governed, and a place of interstate competition and potential conflict. There is widespread concern among states over strategic competition in cyberspace, including cyber espionage and cyber attack. Asia, with its political tensions, vigorous economies, and lack of strong multilateral institutions, is a focal point for this competition. The rise of China and its extensive cyber capabilities defines strategic competition in both Asia and in cyberspace globally.

The cyber domain is better understood in terms of competition than of war. The possession of advanced cyber attack capabilities has tended to instill caution in nations. Still, because of the newness of technology, lack of agreement on norms, and potential to mistake cyber espionage for military action, cyber competition can increase risks of miscalculation, conflict and escalation during wider interstate tension.

The strategic cyber challenge in Asia should be addressed in multiple ways. Cooperation in cyber defence between the United States and its allies can proceed in tandem with greater efforts at US-China dialogue and reassurance. Cooperative approaches worth pursuing include agreement on norms for responsible state behavior in cyberspace and reaching common agreement on the applicability of international laws of war in cyberspace.

Overview

The internet shrinks distance and make borders more porous. It is part of a set of new technologies that form a man-made environment called cyberspace. Cyberspace connects nations more closely than ever before. These close connections provide a new means for both states and individuals to share, influence, intrude and attack.

Conflict and competition in cyberspace is part of a larger shift in the international security environment as power flows away from Europe and as the global institutions developed after World War II are challenged by new economic powers. A new, multipolar order is emerging. The United States is likely to remain the only country with global reach, but “rising” nations – China, India and others – will expand their influence, sometimes in cooperation with the U.S., but at times in competition for influence and regional leadership. The terms of this competition will be not be narrowly military, but will include a contest to influence and control the structures and rules of global finance and business.

Asia is a flash point for cyberspace: The information technology industry is now largely Pacific-based with Asian countries, the United States, and India creating most digital products. The internet is an enabling technology for global business that has helped propel rapidly growing Asian economies. It creates new interconnections and linkages that provide economic opportunity. Asian societies have been enthusiastic adopters of the internet and have made it an important vehicle for political expression within and between Asian nations. Cyber competition and conflict has a large Asian dimension: in this region it encompasses planning for military competition and asymmetric warfare, engagement in economic espionage to gain long-term economic and trade advantages, as well as a new kind of transnational mass political action.

The rise of China defines strategic competition in cyberspace: Information technology and cyberspace occupy a central position in Chinese politics, strategy, and economic policy. China has pursued asymmetric military advantages for more than a decade and is modernizing its military forces for “informatized” warfare. Economic espionage in cyberspace is routine in China and Chinese government agencies, companies, and individuals have increased efforts to illicitly acquire technology or gain business advantage. China’s use of cyberspace to gain military and economic advantage is one of the primary forces shaping a new Asian strategic environment. At the same time, China itself is deeply concerned about the risks of malicious activity aimed against it in cyberspace.

The hierarchy of Asian cyber powers does not always mirror the wider power balance: The “cyber powers” of the Asia-Pacific region are the United States, China, Russia, Taiwan, North and South Korea, and Australia. All are wrestling with how to adjust their policies and practices to new technology and the changes it has unleashed, so the hierarchy of cyber-power will be dynamic and will depend on their and other nations’ continued adaptation. Other countries, such as Japan and India and even less developed nations like Burma are exploring military cyber capabilities, making this a crowded field for competition.[1]

There is continuous interstate competition in cyberspace but this is not war: We have not seen warfare – in the sense of using cyber techniques to damage or coerce other nations – in cyberspace. The same constraints that apply to the use of physical force among nations also apply to cyber attack. Because of the newness of technology, the lack of agreement on norms, and the potential to misidentify an espionage exploit as the opening phase of a military action, cyber conflict entails a greater risk of miscalculation and inadvertent escalation of conflict. This makes all the nations that currently possess advanced cyber attack capabilities cautious. Moreover, among the cyber-capable nations of Asia, there are some shared interests alongside the many areas of potential competition.

FROM CYBER CRIME TO CYBER COMPETITION

Blurred boundaries - crime, espionage and cyber ‘war’

An obstacle to managing cyber competition among states is the blurred boundaries between cyber-crime, cyber-espionage and cyber-attack among states. If the threat of cyber war is exaggerated, the risk of cyber espionage and cyber crime is vastly under-appreciated. Rampant cyber espionage in Asia is a source of instability. The most damaging aspect of cyber-spying is economic espionage - where technology, research products, confidential business information, and intellectual property can all be stolen. The damage may not be visible immediately - but then the goal of espionage is not to be detected.

Espionage is the illicit extraction of information; cybercrime is the illicit extraction of money. These activities are at the core of malicious activity in cyberspace. The internet eliminates the need for physical proximity or interpersonal exchanges, reducing risk and cost for

[1] United Nations Institute for Disarmament Research, “Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization,” 2011, http://kms1.isn.ethz.ch/serviceengine/Files/ISN/134215/ipublicationdocument_singledocument/9b169842-9151-454e-a469-44ac39346672/en/pdf-1-92-9045-011-J-en.pdf

espionage and crime. Espionage and crime overlap in cyberspace, particularly given the use of proxies (cybercriminals who act at the direction of a government). The internet allows the collection of signals intelligence without the requirement for bases, satellites, ships, or aircraft. This provides a global capability to countries that previously had only a regional or national presence. Hacking incidents against the G-20 and the International Monetary Fund (where confidential information prepared for meetings of world leaders was extracted) highlight the potentially strategic consequences of cyber espionage and crime for global political and economic activities.

The most damaging aspect of cyber-spying is economic espionage - where technology, research products, confidential business information, and intellectual property can all be stolen. The damage is usually not visible immediately in an economy - but then the goal of espionage is not to be detected.

The level of cyber crime is likely to grow in Asia and this will increase instability because of cybercrime's links to espionage and military activities. Cyber criminals go where there is money. As Asian countries become wealthier, fraud and extortion committed over the internet will increase.[2] Cooperation among Asian countries in combating cybercrime may be, in some ways, easier to obtain than cooperation in the other areas of cybersecurity that are more closely linked to state power and competition, but the utility of cyber crime as a proxy for pursuing state goals could also limit the scope of any agreement and compliance with it.

From a legal and political perspective, the distinction between armed force, espionage, and crime is very important for decision-making. Crime, even if state sponsored, does not justify a military response under existing international law. Nor does espionage justify an armed response. Espionage and crime can be very damaging, but countries do not go to war over it. Nations who support cyber crime and engage in cyber espionage appear to be careful to stay below the threshold of what could be considered the use of force or an act of war. However, malicious cyber actions can be transnational, with an exploit carried out by hackers in one country against computers in another. This complicates any potential defensive response to cybercrime or espionage as the 'agent" may not be physically present, often cannot be detained, and at times cannot even be clearly identified.

Private actors and proxies

The profusion of private actors in cyberspace, their access to technology, and their ability to engage in illegal transnational acts from their home location, complicates the analysis of cybersecurity. Those with hacking skills – the ability to implant malware or access a computer or network without the owner's permission - are joined by activists who use the internet for political exploits. The line blurs as many activists have the skill to engage in low level hacking and some high-end hackers also have political agendas.

The most dangerous private actors can also operate as proxies -- irregular forces who

[2] Language difference provided something of a shield in the past, particularly for nations like Japan, but this appears to be changing. Asian nations lag in developing consistent cybercrime laws, although ASEAN and other regional organizations have efforts underway to expand and improve legal structure and law enforcement cooperation and Interpol will create a "global complex" in Singapore to "remain one step ahead of transnational criminals by relying upon high-tech crime expertise." Interpol, **"**INTERPOL Global Complex in Singapore to enhance and strengthen policing worldwide,"
https://www.interpol.int/Public/ICPO/PressReleases/PR2010/PR052.asp

undertake action at the behest of the state. Russia and China use proxies to conduct cyber espionage and engage in politically coercive acts. Hackers and cyber criminal communities in both countries are tolerated, co-opted, and at times assisted in their hacking and criminal activities against other nations. The Russian government utilizes its extensive and deep relationships with criminal groups to gain advantage in cyberspace. China's cyber espionage strategy combines both official programs and the coordination of unruly efforts of thousands of individuals, companies, and civil agencies as intelligence collectors. This broad, diffuse, cyber espionage collection program reflects the traditional Chinese approach to intelligence collection – instead of relying on officers operating under official cover, China's approach has been described as "a thousand grains of sand," where businessmen, researchers or students are asked to collect information when they visit a country.[3]

The result of this blend of forces is that malicious cyber activity in China encompasses official programs, independent actions by agencies and companies not directed by the central government, and criminal activities by individuals (who can sometimes act at the behest of some larger entity, a company, ministry or the central government). The central leadership in Beijing does not control all of these actors and it is not clear that it could control them if it wished to do so, despite strenuous efforts to keep internet freedom in check.

Netizens, stability and Asian security

However, Russia and China also worry that the proxies they have created for espionage and attack could turn against them.[4] This fear reflects their own political fragility. Dissent is much more threatening to these regimes than to democracies. While we should avoid overstating the internet's effect in places like Egypt or Tunisia, the internet can greatly expand participation in the political process and amplifies and strengthen political trends in ways that are difficult for authoritarian regimes to manage. This helps explain the neuralgic reaction in both countries to the "Jasmine Revolution" and "Arab Spring," as the regimes fear the growing but uneven power of "netizens" and how it could affect regime survival.

Netizens are not hackers; they are individuals who express themselves in chatrooms, online publications, and blogs and, unlike hackers, they do not illicitly access other computer networks. Their influence affects policies and, perhaps, political stability in China. The "netizens" have political influence. The more skilled among them – and this numbers in the tens of thousands – can easily evade the Great Firewall. The ebb and flow of Chinese politics means that at some times and on some topics, the more extreme voices will be suppressed, but at other times, they will be tolerated or even encouraged. The internet has introduced new forces into Chinese politics that lie outside of the Party's control. Hacktivist activities can influence or inflame public opinion. This is a source of serious concern in China, which has created its own "Fifty Cent Army" of patriotic bloggers who post positive comments about Chinese policies.

[3] See, for example: Northrop Grumman Corporation, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf and Inkster, Nigel, Chinese Intelligence in the Cyber Age, IISS, http://www.iiss.org/publications/survival/survival-2013/year-2013-issue-1/chinese-intelligence-in-the-cyber-age/

[4] Soldatov, Andrei "Vladimir Putin's Cyber Warriors," http://www.foreignaffairs.com/articles/136727/andrei-soldatov/vladimir-putins-cyber-warriors

China's netizens can also affect relations among Asian states in destabilising ways not directed or desired by governments. They form part of a larger political interaction among citizens of China, Taiwan, Korea and Japan. The internet provides a platform for transnational political expression. Some go further to engage in rudimentary hacking (usually website defacements – what we could call digital graffiti), emboldened by the relative anonymity and the absence of physical constraints in cyberspace . The internet can be an outlet for nationalist sentiment that in its most extreme form, can increase the risk of conflict,[5] as governments feel the need to respond to the domestic political pressure generated by internet activities. This is a new factor in Asian relations and carries unpredictable consequences for regional stability.

Most hacktivists do not have the capability to engage in sophisticated cyber exploits, and it is important not to overestimate their political influence. Their effect can be evanescent, with protests springing up quickly and then just as quickly dying down. Hacktivism is a barometer of public attitudes, but there is also the possibility that these new political actors will complicate efforts to predict or manage national responses during a crisis by injecting intense pressure into policy debates. China's decision to first encourage the expression of nationalist sentiment during the 2001 Hainan Island EP-3 episode and then stifle it when its intensity began to foreclose policy options and threaten unwanted escalation, is a good example of the problem of controlling popular sentiment once ignited. The existence now of netizens and social media means that this kind of challenge will be magnified and accelerated in future such crises.

CYBER COMPETITION IN ASIA

Asia's cyber hierarchy

The United States, China and Russia have the most advanced cyber capabilities in Asia. These nations build on their extensive and well-resourced signals intelligence agencies and on their military forces. The capabilities of other Asian nations range from nominal to relatively sophisticated, albeit not in the top tier. Judging from public sources, ten Asian nations- 12, if we count Russia and the United States - are developing cyber capabilities. Eight are developing military capabilities and doctrine – Australia, China, North Korea, India, Malaysia, Myanmar, Japan, and South Korea. Brunei and Singapore -are developing defensive capabilities.[6] Australia has a unique advantage in cyber capability development given its close intelligence-sharing relationships with the US and UK.[7]

The number of countries developing cyber capabilities is not in itself worrisome. Cyber attack is a new military tool that, like aircraft, will eventually be part of every nation's arsenal. Cyber espionage will extend current intelligence activates into a new domain – most countries already monitor domestic telecommunications and those who have active foreign intelligence programs will avail themselves of cyber techniques. In itself, this extension of military and intelligence activities into cyberspace will not radically change power relationships among Asian states.

[5] Nigel Inkster, China in Cyberspace, Survival, July 2010; Hughes, Christopher R. (2000) Nationalism in Chinese cyberspace. Cambridge review of international affairs, 13

[6] UNIDIR, Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization

[7] Gary Waters (ed.), Australia and Cyber-warfare, Australian National University, http://epress.anu.edu.au/sdsc/cyber_warfare/pdf/whole_book.pdf

China as a strategic competitor: cyber conflict and cyber espionage

As with so many other security issues in Asia, cyber security revolves around the rise of China. China's growing strength and its desire for increased regional influence (if not dominance) is the principal strategic issue for Asia. This growth has set in motion a process of reaction, accommodation, and adjustment - the chief issue being whether China's "development" will be peaceful or aggressive. This reflects internal Chinese differences over a continuance of the approach originally put forward by Deng Xiaoping which avoids confrontation, and those who wish now to take a more assertive stance. This internal debate shapes how China adjusts its own actions and policies to better fit its new and more important place in the world. The internet complicates this debate because China's leaders must also deal with the growing but uneven power of China's "netizens" to affect policy-making.

China is redefining its relationships with other Asian nations. China's expects that it will gain influence, if not deference, to its leadership. The rise of China means that other Asian nations must decide where to accommodate and where to confront a newly powerful China with aspirations to restore its regional position and power. In turn, China's leaders must decide where an acceptance of international norms and systems best serves China's interest and where challenging the existing order provides greater benefit. This is a dynamic policy, the subject of internal debate and calculation in Beijing and other capitals. The most influential elements in Chinese thinking appear to include the development of asymmetric military capabilities, promoting indigenous innovation, and to restoring China's rightful place in the world after the "Century of Humiliation."

Information technology and cyberspace have become essential elements in Chinese politics, military strategy, and business. China uses cyber techniques to redress what it sees as an imbalance of power, using cyber espionage to compensate for its technological lag and weak national innovation capability, as well as an element of a larger strategy on how to gain advantage in any military conflict.

The use of cyber technologies is a central element of the strategic competition between China and the US, and in China's efforts to gain advantage over potential regional competitors like Japan. If China was not actively engaged in malicious cyber activities, cyber security and cyber conflict would have a much lower profile and be of much less concern both regionally and globally. Cyber conflict could become a significant and damaging factor in China-US relations as it involves and exacerbates both economic and military competition.

China's military emphasizes both modernization (which includes a heavy emphasis on the use of information technology - "*local* wars under *conditions* of *informatization*") and the achievement of asymmetric advantage over the US by various means, including cyber attack[8]. Asymmetric attack strategies that would use cyber techniques (perhaps in combination with other modes of attack, including electronic warfare and anti-satellite weapons) may appear to give the Chinese some military advantage. Still, it is worth considering whether the Chinese military overestimate this military advantage in ways that could be potentially destabilizing in pre-conflict situations[9].

[8] See, for example, US China Commission, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage." http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf

[9] For an early but still useful account, see Qiao Liang and Wang Xiangsui, 1999, Unrestricted Warfare, Beijing:

Cyber economic espionage

China's intelligence activities in cyberspace are an element of a larger economic espionage program that focuses on illicit technology transfer. This program began when Deng Xiaoping decided to let foreign companies begin manufacturing in China. China's economic espionage originally depended on domestic activities including communications monitoring and human collection, but cyber capabilities now give the program a global reach. There are at least three cases of large, complex economic espionage operations aimed at western companies originating in China that have been uncovered in recent years. Often these programs incorporate political motives such as acquiring information on the Dalai Lama or on human rights activists.[10] Agents working in US defense companies are another source of access to technology.[11] China's cyber espionage acquisitions may not radically shift the balance of military power, but indicate a competitive and possibly hostile attitude towards the United States.

There are reasonable grounds for concern over the loss of advanced military technologies. China was able to improve its nuclear submarines in about half the time it took the US or Soviet Union to. China's J-20 "stealth" fighter aircraft appeared more rapidly than experts had expected. Aerospace, sensor, naval, and stealth technologies have been targets of Chinese acquisitions efforts. A decade ago, for example, foreign hackers intruded into the computer networks at US military research facility engaged in work on stealth technologies. China was suspected in these intrusions. If technology was illicitly acquired, a lag of several years would be expected before it could be exploited and deployed in the acquiring country.

This is suggestive of possible advantages that have accrued to China. There are interesting parallels between China's five-year economic plans and cyber espionage activities that appear to have originated in China. As part of its larger strategy to create a national information technology industry, China has long sought to acquire the means to develop an indigenous computer central processing unit (CPU). Intel Corporation, the world's leading producer of CPUs, was a target of a January 2010 corporate hacking (which also involved Google). If Intel lost intellectual property to China in that incident, it could take many years to turn any information acquired into a working CPU.

China is perhaps the leading practitioner (although by no means the only practitioner, in Asia or globally) of economic espionage in cyberspace. Chinese government agencies, companies, and individuals have expanded their efforts to illicitly acquire technology or gain business advantage into cyberspace. During a trial of executives from the Australian mining company Rio Tinto, hackers from China reportedly made over 200 attempts to break into the defense team's networks. The head of the British Security Service warned companies that

PLA Literature and Arts Publishing House, http://cryptome.org/cuw.htm; see also Gurmeet Kanwal, "China's Emerging Cyber War Doctrine," Journal of Defense Studies," Institute for Defense Studies and Analysis, 2008

[10] Publicly reported example of espionage activities include exploits called Ghostnet , Aurora, and a network operating in Belgium http://www.spacedaily.com/news/china-05zw.html; Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee. August 2011; Information Warfare Monitor, University of Toronto, Tracking Ghostnet: Investigating a Cyber Espionage Network, March 2009

[11] See, for example, http://www.washingtonpost.com/wp-dyn/content/story/2008/04/02/ST2008040204050.html; http://www.smh.com.au/world/us-judge-tells-china-to-stop-sending-its-spies-20100209-npss.html

hacking has become a routine business practice in China.[12] Chinese officials tolerate malicious activity against foreigners and routinely use non-governmental hackers as proxies. However, Chinese companies are as much a target as firms in other countries for cyber espionage.[13] China's cyber espionage reflects Chinese attitudes toward the protection of intellectual property. Currently there is no comprehensive protection of intellectual property in China. That said, there is a growing realization in parts of the Chinese government that the lack of strong IP protections does serious damage to China's ability to innovate. Chinese views on intellectual property are also important in determining the scope of cyber conflict. China's generally weak protections for intellectual property have migrated into cyberspace, with consequences for China's own indigenous innovation efforts (it is a disincentive to innovate if others can steal your innovation investment without penalty). There have also been consequences for China's economic and technological competition with other nations (particularly the United States, Japan and Korea).

Cyber advantage China?

In general, the expansive use of cyber techniques for economic espionage means that cyber conflict works to China's advantage when compared to the US or other Asian nations. China has integrated the use of cyber techniques into its military doctrine and economic policies far more comprehensively than any other nation in the region. Japan and Australia have focused more on cyber defense. North and South Korea do not yet have the capabilities to engage in the high end of cyber conflict – the ability to inflict physical damage through cyber attack. As Southeast Asian nations gain access to high-speed networks (which allow for easy access across borders and the ability to transfer large amounts of data in a very short time) there has been an increase in low-level cyber crime. However, the only other nation that comes anywhere near China in using cyber techniques for espionage and military advantage is the US.

Although the US and China are "near-peers" in terms of some cyber capabilities, there are crucial differences. The US government does not engage in economic espionage and intellectual property laws are more strongly enforced in the United Sates than in many other countries, including China. Nor are American political "hacktivists" encouraged by the US government. The US approach to cyber conflict treats cyber techniques as traditional tool of statecraft, providing advantage in military and political intelligence, and as a new weapon to strike opponents.

The US uses cyber techniques to monitor and assess Chinese capabilities and intentions, and to gain battlefield advantage in the event of conflict. US cyber actions, unlike Chinese cyber actions, are focused on their competitor's official government activities and not on economic espionage. US laws effectively preclude economic espionage by government agencies and punish private individuals who breach intellectual property laws. In any event, the U.S. sees little need to steal technology that it regards as inferior to its own.

Any effort to assess how much of a contribution cyber espionage makes to China's military and economic power must necessarily be speculative and anecdotal. Acquiring intelligence does not always mean that it is used, and there is usually a lag between the acquisition

[12] Times of London, "Jonathan Evans alert on China's cyber spying," December 1, 2007 http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece

[13] Office of the National Counterintelligence Executive, "Foreign Spies Stealing Us Economic Secrets in Cyberspace, October 2011, http://www.dni.gov/reports/20111103_report_fecie.pdf

(measured in years) of technical information through espionage and the ability to deploy it. In general, cyber espionage accelerates the increase in China's power vis-à-vis other Asian nations and China's own technological and economic growth, but it is by no means the major contributor to China's growth, which is the result of the reallocation of productive assets, the influx of foreign direct investment, and access to the global market on favorable trade terms.

Cyber espionage provides China with an intelligence benefit through an increased understanding of US intentions, strategies, and capabilities, but it is in economic espionage against the U.S. and other Asian nations where China's main advantage lies. While the US also gains tremendous intelligence benefits from cyber espionage, the "net balance" of the exchange between the US and China in cyber espionage favors China. China is more vulnerably politically to the free flow of information over the internet, the U.S. is more vulnerable to economic espionage, and this may put it at a disadvantage in a competitive cyberspace environment.

Or China the vulnerable?

A number of caveats need be attached to the assertion that cyber competition favors China. Intelligence successes do not always translate into better performance. Leaders may discount or misinterpret new information that does not fit with their existing concepts or views. Industrial or scientific establishments may not have the capability to exploit fully technical intelligence. In rare instances, the target may introduce false information in order to mislead an opponent. These factors hamper China's ability to benefit from cyber espionage.

The politics of cyber security in China are not monolithic; agencies and interests groups compete with each other to influence policy. Decision-making in China on cyber issues is fragmented and stove-piped, with little coordination among agencies or between the security and economic agencies. The Chinese have no equivalent to the US National Security Council to ensure policy coordination. This lack of coordination increases the risk of miscalculation in any conflict.

China's networks are fabulously insecure – the widespread use of pirated software guarantees that they are easily and routinely penetrated. China's primary cyber security concern is to prevent challenges to Party rule and to maintain control of information, but there is also concern over China's own exposure to hacking and cybercrime from both domestic and foreign sources. Chinese officials worry that that the creation of the US Cyber Command may put them at a military disadvantage and they have a long-standing fear that a reliance on US technology creates vulnerabilities in Chinese systems.

The Chinese perceive Cyber Command as part of a larger US effort to dominate cyberspace. They believe that the US is developing powerful cyber strike capabilities for use against China. Some Chinese officials compare US cybersecurity efforts to missile defense, saying that just as missile defense is intended to cancel out China's nuclear deterrent, US cyber security efforts are intended to provide US forces with "impunity" to attack in cyberspace. The Chinese may also assume there is an explicit and coherent US strategy to preserve its commercial and military advantages in cyber space. It is possible that they interpret US actions through the prism of their own beliefs and expectations. This "mirror-imaging" leads them to attribute to the US those things they themselves might do, including a controlling relationship with the private sector, supply chain manipulation, and dominance of internet governance structures for commercial gain and national power.

The Chinese are deeply concerned over supply chain security. They are convinced that the US has built “backdoors” into products like Windows and Intel processors. The Chinese were shocked to discover that Microsoft can remotely access any computer in China that is running Windows.[14] They do not believe that the US does not have the same controlling relationship with American companies that the Chinese government has with Chinese IT companies. Their solution is an intrusive set of measures for inspection (and possible copying) of foreign products for vulnerabilities, and the promulgation of Chinese technical standards and an effort – named “indigenous innovation” – to replace western technology with Chinese products. Successive five-year strategies point to a desire to create a national information technology industry that will supply “made-in-China” products that the Chinese believe will be more trustworthy. [15]

The dilemma with this approach, as the Chinese well realize, is that it could affect the ability to create new products that are competitive in the global market. It could hamper the ability of Chinese firms to compete globally. Chinese cyber security policy reflects tensions between conflicting goals. Economic espionage provides advantage in business and technology, but could put bilateral relations at risk. China wants to create indigenous innovation, but is undecided as to whether to force the use of Chinese technology (which is still inferior) or to cooperate with the west and accept western technologies that may have built in vulnerabilities. Openness brings political risk, but restricting access to information will damage competitiveness in research and business. Two larger issues – how China’s domestic politics will evolve and how China will relate to the rest of the world – shape the internal cyber security debate.

North Korea as a cyber challenge

China is the most active of the cyber powers in Asia, but the greatest potential source of instability in cyber space for Asian nations may come from the growing capabilities of North Korea. While these capabilities are easy to exaggerate, North Korea has been interested in computer technologies for almost two decades. In the mid 1990s, North Koreans assigned to the United Nations in New York enrolled in programming classes, North Korea acquired American computers despite sanctions (often buying them in consumer stores and transshipping them on Air Koryu flights), and North Korean technical institutes began work on microprocessors and technology.

There is undeniable interest and investment by the North, but not yet the capability to launch cyber attacks.[16] North Korea appears to have a very different calculation of acceptable risk to most nations. When it acquires advanced cyber capabilities, the likelihood of cyber attacks that result in destruction or damage will increase.

North Korea has used the internet for propaganda and political purposes in the South, using false names to log onto websites to post pro-North opinions, for example. Yet the North faces many difficulties if it seeks to become a cyber power. It does not have routine access to

[14] “Tang Lan” Let us join hands to make Internet safe,” China Daily, February 7, 2012, http://www.chinadaily.com.cn/usa/epaper/2012-02/07/content_14551811.htm

[15] James A. Lewis, “Building an Information Technology Industry in China: National Strategy, Global Markets,” CSIS, May 2007;

[16] James A. Lewis, “Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace,” 38 North, September 7, 2010, http://38north.org/tag/cyber-war/

advanced technologies. North Korea will not be able to use the proxy strategy followed by China, where private hackers carry out state instructions, operating as irregular forces or mercenaries. Most importantly, North Koreans do not have the untrammeled access to the internet that sustains hacking communities and skills. North Korea has begun to take steps to move away from its reliance on external service providers, buts its technological and political cultures remain obstacles to developing strong hacking capabilities.

That said, if the political situation in North Korea continues to invest in building advanced cyber capabilities, it will eventually acquire them. Should the North acquire cyber attack capabilities, these will likely be in reserve primarily as an adjunct to armed conflict. However, there may well be continued acts of calculated provocation, tied to internal DPRK politics and intended to manipulate the US, South Korea or other countries. There will likely be a strong temptation to use cyber techniques – causing blackout or other service disruption as a way to emphasize Pyongyang's displeasure. We know little of North Korea's decision-making process, but the already large possibility of miscalculation inherent in cyber could be amplified in the closed processes of the North.

REDUCING TENSIONS IN CYBERSPACE

To recapitulate, this analysis has emphasized: that there is a continuum from cyber-crime to espionage and other forms of cyber-competition exists in Asia; that much of this is China-centric; that these activities do not constitute war; but that cyber-competition can add to the risks of conflict occurring and serve as an adjunct to force if it does. It is important, then, to consider possible ways to manage or mitigate the risks of intensified cyber competition or conflict in Asia.

These risks can better be managed if cyber conflict is put into a framework of shared understandings on norms of behavior and the application of international law. Controlling this risk requires establishing "rules of the road" in cyberspace – on state behavior, understanding on military intention, and cooperation on cybercrime - common understandings on acceptable behaviors and norms.

Asia's relatively weak institutions for international security cooperation do not bode well for effective discussions on these issues at an inclusive region-wide level. Existing multilateral vehicles for discussion in Asia – whether ASEAN-centric institutions like the ASEAN Regional Forum or the East Asia Summit, or perhaps APEC - may be inadequate to the task. One alternative would be to await global understandings on cyber conflict to reduce the chance of cyber conflict in Asia. There are several "global" efforts to reconsider cyberspace governance and cyber security already underway, including work in governmental expert committees in the ITU and in the UN.

Another alternative would be bilateral discussion between the US and China. The new emphasis in American policy is on engagement, on collective defense of cyberspace with allies, and the development of norms for responsible state behavior.[17] A"G-2" approach has some appeal - cyber security issues have been raised at both the 2011 Security and Economic Dialogue and in recent meetings between Barrack Obama and Xi Jinping. While bilateral discussions are essential, the US also needs to work closely with its regional partners, acting

[17] The White House, "International Strategy for Cyberspace," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

as a proxy for their interests and bearing mind that any understandings with China will need to ultimately be implemented on a regional and global scale.

Serious cooperation on cyber security may have to begin in the three separate bilateral security arrangements the US has with Australia, Japan, and the Republic of Korea through which increased cooperation in meeting the cyber threat can be made. The close intelligence and defense relationship with Australia led to agreement to amend the existing mutual defence treaty to include cyber security[18]. Improving relations with India also offer some scope for collaboration, particularly since India is concerned about Chinese cyber activities[19]. As with other security issues in Asia, China's activities have created an implicit commonality of interests among other regional powers. China has misplayed a series of maritime incidents in its relations with several other nations, and it has battered Australia, Japan, India and the United States with an unending stream of cyber espionage intrusions into both private and governmental networks.[20]

This creates a powerful incentive for cooperation and collective action. However, negotiations to create collective defence in cyberspace among Asian nations would exacerbate Chinese fears of encirclement or containment by the US and its allies. Cooperative actions among like minded nations will improve cybersecurity, but will need to be balanced against the possible expense of increased regional tensions.

The most important way to assure China, reduce its suspicions and at the same time restrain its malicious activity in cyberspace is through engagement and confidence building. China asked to include cybersecurity on the 2011 Strategic and Economic dialogue (S&ED) agenda - an indication of their interest if not concern. The US and others can engage China to establish clearer understandings of state responsibilities in cybersecurity (as was done in the 1990s on nuclear non-proliferation) and further development of cooperative measures – CERT-to-CERT arrangements or the sharing of certain kinds of threat information. Military exchanges would also be useful, but these would need to take place outside the US-China relationship as US military defence officials report that the PLA is unwilling to engage them in dialogue on this issue.

The scope of cooperation with China depends, in good measure, on how Chinese cyber policies evolve. Key decisions for China include deciding when the costs and risks of its cyber espionage programs outweigh the benefits, whether the use of proxy forces (which can be difficult to control) increase the risk of conflict, and, how to direct internet activities so as to accommodate the growing political power of China's "netizens" without compromising the Party's control.

An important obstacle to agreements to manage cyber competition or prevent cyber conflict is differing national priorities with regard to access to information. In negotiating international agreements on cyberspace, democratic nations will seek to limit espionage and crime. Authoritarian countries may instead seek to limit access to information and to social networks which they see as weapons that can be used against them. Both China and Russia believe the US uses information as a weapon to destabilize their governments.

[18] Reuters, "U.S., Australia to add cyber realm to defense treaty," September 14, 2011

[19] Deepak Sharma, "China's Cyber Warfare Capability and India's Concerns," Institute for Defense Studies and Analysis, June 2009, www.idsa.in/system/files/jds_5_2_dsharma.pdf

[20] For a list of major cyber incidents, see Center for Strategic and International Studies, 'Significant Cyber Incidents Since 2006," http://csis.org/publication/cyber-events-2006

Announcements that the US will fund technologies to circumvent internet restrictions only encourage this belief.[21]. The experience of the Orange Revolution in Ukraine, dissent in Iran, and the more recent "Arab Spring" events in Tunisia and Egypt reinforce the notion that new technology creates political risks that the US will seek to exploit. One Chinese official stated in private meetings that "Twitter is an American plot to destabilize Iran" (and by implication, China). It is difficult to see how these ingrained suspicions can be overcome in the near term.

Asian nations and the US must decide whether to emphasize engagement or confrontation in their approaches to China. It is possible to pursue both strategies simultaneously up to a point, as both seek to change how China interacts with its neighbors. One change in recent years is that smaller Asian nations have been willing to take a more confrontational stance towards China (best exemplified at the multiparty July 2010 regional security discussions in Hanoi). They may feel empowered by the US military "pivot" to Asia or they may feel the need to counter Chinese pressure. Some larger Asian nations, such as India and Japan, will experience greater strains in their relations with China irrespective of US actions.

China's own sensitivities and the attitude of its military increase the risks of tension with other nations. We have seen "near misses" in the EP-3 incident and maritime disputes with Japan and Vietnam. Tensions over the Paracel islands and other disputed waters are a potential flashpoint. Unconstrained malicious activity in cyberspace, combined with the ability of "hacktivists" to whip up nationalist sentiment and insult counterparts in other nations could exacerbate any crisis. The potential for malicious activity in cyberspace to inflame or accelerate existing tensions, or to increase misperception or miscalculation among governments of the intent and risk of cyber actions, poses the greatest cyber risk to security in Asia.

It is in no one's interest to see cyber conflict – espionage, theft, and political action – escalate into a military clash or lead to a breakdown in trade. However, nations are reluctant to admit to possessing offensive capabilities. They believe this provides a measure of deniability, but the illusion that ones actions are secret when they are not only exacerbates distrust. Attribution of the source of a cyber attack is difficult, but this difficulty is overstated. The hope that an attack would not be correctly attributed may lead to destabilizing miscalculation; it is a weak shield for a nation to hide behind. It is natural for governments not to admit to espionage, but clearer understandings on military doctrine, the use of proxies and on the limits of industrial espionage could lower tensions created by cyber conflict. Other cooperative approaches include agreement on norms for responsible state behavior in cyberspace, agreeing not to supply or train terrorists in the cyber domain, and reaching common agreement on the applicability of international laws of war in cyberspace.

We are used to considering the contribution of intangible factors and clandestine activities to interstate competition and conflict, and to gauging their effect on national power. Cyber activities greatly expand the scope for such actions. Global information networks connect 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. Given that cyber conflict occurs on a global network, it is hard to "regionalize" it, but just as Asia has become the most dynamic venue for global economic activity, so has it also become the locus of cyber conflict.

[21] Robert O. Freedman, 2011, "The Arab Spring's Challenge to Moscow" in Journal of International Security Affairs, Fall Winter No. 21