SITC Study of Innovation and Technology in China 科技创新 AN IGCC PROJECT

IGCC University of California Institute on Global Conflict and Cooperation

The United States Naval War College Viribus Mari Victoria

China and Cybersecurity: Political, Economic, and Strategic Dimensions

Report from Workshops held at the University of California, San Diego April 2012

Contact:
Jon Lindsay (jrlindsay@ucsd.edu)

Contents

Executive Summary

China and the United States, the two largest economic powers in the world, depend upon global cyberspace for their economic productivity, social livelihood, and national security. Both governments and industry have become increasingly concerned about the safety and reliability of their information systems, but there remains great uncertainty about the true nature of risks and the best ways to address them. Western audiences in particular have had little exposure to Chinese perspectives and politics which influence these issues.

The University of California Institute on Global Conflict and Cooperation and the U.S. Naval War College recently sponsored two workshops; these brought together Chinese and Western scholars, policy analysts, and scientists to discuss the political, economic, and strategic dimensions of cybersecurity in China. Their research findings, many of which are summarized in this report, span a wide variety of topics and interpretations, as should be expected from a policy issue spanning industrial regulation, law enforcement, military strategy, and civil rights concerns. They highlight areas of common concern as well as controversy.

Cybersecurity and Mistrust in U.S.–China Relations

In recent years the security of global information systems has become a contentious issue in U.S.–China relations. U.S. government sources allege that Chinese intrusions targeting proprietary economic data and sensitive national security information are on the rise. At the same time, a large proportion of malicious activity globally originates from computer hosts located in the United States. Both the U.S. Department of Defense and the Chinese People's Liberation Army (PLA) view cyberspace as a new domain of conflict, and they eye each other warily. Nationalist "hacktivism," in the form of website defacements, service denials, and network exploitation, flows both ways across the Pacific. This unfortunate situation exacerbates mistrust and raises suspicions in both countries regarding the others' motives and activities.

Cybersecurity as a Political Economy Problem

There has been growing appreciation in the United States that cybersecurity, while superficially a technical issue, is actually a profoundly economic and political problem. The private sector actors who generate risks often lack incentives to mitigate them, and the public sector has been unable to coordinate policy responses across government agencies with differing priorities. However, Western audiences have had little exposure to empirical research on the corresponding domestic policies, governing organizations, and economic tradeoffs in China. Failure to appreciate China's domestic economy and politics can lead to a profound misunderstanding of its international activities. It is especially important to understand the domestic civilian context of cybersecurity given that the majority of day-to-day insecurity in cyberspace is economically motivated and risks of all types involve civilian information technologies.

China’s Fragmented Information Security Policy Environment

Contrary to popular perceptions in the United States, China does not have a monolithic, coordinated policy approach to cybersecurity. Although political power is centralized in the Chinese Communist Party, Chinese governance is fragmented regionally and functionally. For civilian or industrial cybersecurity, China has to contend with a complicated tangle of regulatory institutions, inconsistent implementation of policy directives, and public and private sector actors pursuing incompatible interests. At the same time, there is a fractious network of military, intelligence, and other state entities involved in cyber policy and activity who are concerned about international as well as domestic security.

The United States and China do indeed have different perspectives on the nature of risks to and through cyberspace. These include differences on the degree to which “information security” should include controls on Internet content, and about the ideal policies for regulating their information networks. Nonetheless, they are similar in that domestic political and economic factors in each state loom large for the dynamics of cybersecurity, complicating efforts at domestic and international policy coordination. Cybersecurity experts in both countries experience frustration in trying to elicit a coherent policy response from their governments.

Growing Domestic Chinese Cybercrime

China’s networks face a variety of idiosyncratic risks, such as ballooning levels of domestic cybercrime, widespread dependence on Western software, and uneven legal regimes and enforcement. While cybercrime has been on the rise around the world, it exhibits some interesting characteristics in China. There is a large underground market targeting virtual goods such as video game accounts and currencies in which both the criminals and the victims are Chinese; by contrast, cybercrime from Eastern Europe targets victims in Western Europe and the United States, avoiding domestic predation. Chinese cybercriminals exploit online forums to buy and sell their goods, whether stolen assets or hacker infrastructure, and lax law enforcement means they are often quite open about it; this makes some promising research possible for researchers who have a native command of the jargon which criminals use.

Diverse Ideas about and Approaches to Information Warfare

On the national security front, both states are in a period of experimentation with how best to conceive of and adapt new technical possibilities in cyberspace to support their national security interests. There has been vigorous debate in Chinese defense intellectual circles about the nature of information warfare, inspired by a number of different influences, sometimes similar to perspectives of other nations, and sometimes unique to China. As in the civilian cybersecurity sector, the implementation of these ideas by various military, intelligence, and civilian militia organizations is not systematically integrated.

Active Cyber Exploitation from China

Data available through analysis of cyber penetration patterns, timelines, and forensic artifacts allow us to assess with confidence that many private firms and government organizations in the United States and elsewhere are being targeted for intelligence collection originating from China. Sometimes there is evidence that enables researchers to identify particular individuals, as in the Night Dragon episode, but often it is not possible to determine whether state organs are actively involved, tacitly supporting, or just unable or uninterested in intervening. There remain many mysteries about the level of involvement of different parts of the Chinese state—military, intelligence, or otherwise—in potentially risky activity. U.S. cyber offensive and intelligence capabilities, likewise, are shrouded in mystery.

Promote Future Dialogue and Research Collaboration

Resolving uncertainties should be a priority to reduce potentials for misperception, and to thereby dampen spirals of mistrust. First, there is uncertainty about what types of capabilities exist or are emerging in which organizations. Second, there is uncertainty about what these capabilities might actually be useful for in the broader strategic and political context.

"Track II" dialogues among scholars, scientists, and industry offer a promising avenue to 1) improve mutual understanding of the key technical, economic, and strategic challenges in this area; 2) clarify national and industrial perspectives; and 3) share ideas on how to improve domestic and global management of cyberspace. We are impressed with the open frontier of researchable topics regarding China and information security, both in terms of availability of open-source data in Chinese and interest among all parties in gaining a better understanding of it. We look forward to ongoing future discussions and collaborative research.

National Cybersecurity Policy

Cyberspace Security and International Cooperation in China

Li Yuxiao, Director of the China Internet Governance Research Center,
Beijing Posts and Telecoms University

Experts have predicted that in the mobile Internet era, the most terrible problem will be security, and this prophecy is now becoming a reality. In recent years, Internet websites, as well as the related value-added telecommunications business, are booming, and the business scale, the number of users, and social influence are increasing. Because of a lack of risk awareness, sense of responsibility, and necessary protective measures, the disclosure of users' information, website attacks, and other incidents have occurred casually. Some of them have even caused serious harm and negative effects.

In 2011, about 8.531 million computers in China were attacked by rogue programs every day, which accounted for 5.7 percent of daily networked computers, reaching a growth rate of 48 percent compared with the year of 2010. According to an assessment report recently published by China's Software Test Center, a sample of bank websites got only 31.98 points (the full mark is 100 points) in an evaluation survey, which was the lowest score. In addition, another survey showed that 60 percent of 2500 persons had their personal information stolen; more than 66 percent of them agreed that we should intensify efforts to combat the illegal behavior.

Accordingly, we can see that China's situation of Internet information security is quite severe. The phenomenon of information leakage under the environments is serious, so the protection of privacy and personal data should be strengthened. Internet abuses are unscrupulous. There is a lack of protection for privacy and data. There are legal loopholes in public information safety, and China lacks an effective management mechanism.

The deep reasons for the situation are as follows. China's current emphasis on information security is not enough. Its institutions and the legal system are incomplete. Information security strategies and plans are insufficient. Internet technologies need further development. General public education is barely satisfactory. Further international cooperation is really needed.

Cyberspace security is an common, international problem. We need to face and solve it together. However, there are differences between countries, so it is impossible for all countries to do everything in the same style. Every country has its own problems on Internet security. It is unfair for one country to criticize others according to its own policies. Because the topic of cyberspace security is very sensitive, the discussion is not thorough enough. Governments cannot reach a consensus in some questions. So we need to open "track II" academic cooperation between different countries. Through such cooperation, we can define the basic principles and rules and establish the mechanism to work. Topics we focus on could include cyber security, privacy, and business data protection.

There is an old Chinese saying: Make much of what is common and minimize differences. Cyberspace is boundless, and different countries and nations have tremendous benefits and opportunities in it. We should take measures based on mutual respect and make common developments. When we humans become a whole by using the Internet, our intelligence could work together for developing humanity. We need open exchanges and cooperation to create a win-win situation. We also need to ensure each other's interests and rights in cyberspace. In this process, academic cooperation is very important now, so we need to help to bring about a consensus between academic institutions on the way ahead.

Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy

Jimmy Goodrich, Global Policy Director, Information Technology Industry Council

What motivates China's thinking on civilian national cyber security issues (i.e., on industrial policy rather than military strategy, diplomacy, and information control issues)? Who are the key actors? What are the primary policy initiatives? There is virtually no English language research in this critical area, but information can be found through publicly available Chinese sources.

In Beijing many cyber policies are in "deadlock" while senior leadership is focused on "more pressing matters" and a fragmented constellation of bureaucratic actors aggressively protect their turf. The civilian cybersecurity apparatus is dominated by a professional technically-oriented cadre without deep economic or international relations expertise. The current lack of coordination and leadership has led to a stagnation in policy and calls for a senior coordinator. This state of affairs might remind some readers of U.S. cybersecurity policy.

Chinese stakeholders include the Communist Party, government agencies, the PLA, academia, critical infrastructure operators, and ICT industrial suppliers. Within the Party and State Council, various Leading Small Groups touch cyber issues. The State Informatization Leading Small Group (SILG) for national IT development policy was formed in 1993 and reconstituted in 2001 under Zhu Rongji, but it received less emphasis under Hu Jintao. Its routine work was handled by the State Council Informatization Office (SCITO), but this appears to have been disbanded in 2008, leading to high degrees of uncertainty for many players.

For cybersecurity in particular, the National Network and Information Security Coordination Small Group (NNISCSG) was created in 2002 as sub-group under SILG, although previous ruminations have existed since 1996. The NNISCG is chaired by Li Keqiang, with deputies Zhang Dejiang, Liu Yunshan, Ling Jihua, Meng Jianzhu, and Chen Bingde. This body drafted China's national civilian cyber security strategy ("Document 27") and approved major cybersecurity related policies and national strategies (e.g., the Multi-Level Protection Scheme, China Compulsory Certification, disaster recovery, incident management, e-government security, trusted networks, infosec standards, and the infosec five-year plan). After completing strategy formulation and policy planning in the first part of the decade, this body was disbanded in 2008 and reconstituted in 2009, but there is no public record of meetings since then, and various ministries have a hand in implementation.

The four primary security agencies managing information security are wryly referred to as "Kung Pao Chicken" (宫爆鸡丁), a pun on their names (公安，保密，机要，兵丁). There is little oversight or executive-level review of the security agencies. The Ministry of Public Security is responsible for cybercrime and critical infrastructure protection and has a nationwide network of research labs. The State Encryption Bureau, also known as the CCP Central Office Confidential Bureau and Central Cryptography Commission, is responsible for party, military, and civilian encryption management (but not intelligence cryptology). The State Secrets Bureau, also known as the CCP Secretariat Secrets Protection Office, manages all classified networks and has been very active since the 2009 revision to the state secrets law. The military (PLA) is also a key player in the civilian sphere, through front end elements of General Staff Department units (3/PLA, 4/PLA, PLA Encryption Bureau, and the PLA State Secrets Office).

Slightly less important since the 2008 ministry reorganization which disbanded SCITO, the Ministry of Industry and Information Technology (MIIT) has an information security coordination department and is responsible for telecom and Internet security. The Ministry of State Security prefers a low public profile, but is understood to be the most technically capable, especially in the area of information assurance (administered through the 13th bureau, the science and technology bureau, and CNITSEC). The Politburo Standing Committee for Propaganda is also important.

China's civilian cybersecurity elite is a professional, technically-versed group of individuals. The "first generation" of cybersecurity officials still hold power, with much representation from Chinese Academy of Engineering (CAE) academicians and Chinese Academy of Science (CAS) fellows. Many current officials have been under the tutelage of these senior scholars/officials. Most cyber policymakers have spent time doing technical research in academia, with little experience in economics or international affairs. Patriarchal relationships lead to difficult situations for junior officials.

China's civilian national cybersecurity strategy, released in 2003 and initially classified but later promulgated more widely, is known as "Document 27: Opinions for Strengthening Information Security Assurance Work." It enshrines a principle of "active defense" and sets policy foundations for critical infrastructure protection, cryptography, dynamic monitoring, indigenous innovation, talent development, leadership, and funding. Specific policy initiatives launched through Document 27 have led to an antagonistic system of policy spaces vigorously defended by bureaucratic owners. Any incursion by other agencies or newcomers has led to conflict. Although SILG/SCITO aided initial policy formulation, its disbanding in 2008 led to "chaos" in China's civilian cybersecurity policy arena. These separate policy initiatives include:

- The multi-level protection scheme (MLPS), China's critical information infrastructure protection regulation, which has had tremendous resources invested into implementation and has led to what might be called an MLPS "industrial complex."
- Product assurance is security testing for IT products. Each security agency runs its own certification schemes (CNITSEC/TRIMPS/ISCCC/SSB/PLA), leading to the perverse result that some economic actors forego security assurance altogether. For example, there is widespread non-use of transport layer security—"https"—for Chinese Internet applications. The Certification and Accreditation Administration (CNCA), a newcomer to the infosec space, tried from 2004 to 2008 to create a unified scheme but met opposition at home and abroad.
- Encryption policy predates Document 27 to 1999 under the "State Encryption Management Commission" and includes a number of regulatory schemes to promote domestic encryption for e-signatures, certificate authorities, etc., focusing primarily on government/CCP systems.
- Risk assessment is not a component of other existing policies but instead is implemented in isolation by the relatively underfunded NDRC State Information Center (a former manifestation of SCITO).
- China's infosec standards are run by a committee co-chaired by representatives from the security agencies, known as the China National Information Security Standards Technical Committee (TC260). It is opaque and closed to foreign participants. It has turf issues with CCSA.
- IT security research and development is managed through MOST/NDRC/CAS programs like projects 863/973, the Megaprojects, and the NDRC Industry Development Fund. There is a State Key Laboratory for Information Security under CAS.

Following the 2008 disbandment of SCITO there has been continued implementation of existing initiatives as well as a number of new initiatives that appear to be uncoordinated passive response policies (somewhat like the U.S. approach) for: SCADA security, e-government systems compliance, trusted network connectivity, and botnet/telecoms security. There is a serious lack of progress in CCCi/Product Assurance where interagency cooperation is most needed. Classified systems information assurance is a new focus, with expanded activity from the State Security Bureau (SSB), which seeks to expand its power by keeping other agencies away from "classified systems." The SSB gained vice-ministerial ranking in 2009 and started opening university "state secrets institutes" in 2011 focusing on computer security.

U.S.–China engagement must take into account China's fractured cybersecurity space. Without a central Chinese focal point, dialogue may also be fractured. Focused, issue-based discussions need to be coordinated with the appropriate organizations. The lack of a state council level office complicates MIIT's ability to effectively coordinate and organize a robust dialogue.

Chinese Perceptions of and Strategic Response to Threats in Cyberspace

Cortez A. Cooper III, RAND Corporation

How do Chinese Communist Party (CCP) leaders perceive cyberspace threats, and what is the influence of PRC national development strategy and security policy on them? China's national development strategy is formally promulgated in Hu Jintao's "Scientific Development" dictum, which sets an objective goal for China to achieve the status of a mid-level developed country across its breadth and depth by 2050. The strategy encompasses a whole-of-government approach to building comprehensive national power under CCP control—focused on enhancing and protecting "core interests" related to national sovereignty, security, territorial integrity, and peaceful domestic development. Scientific Development provides a general blueprint for maintaining social stability through steady, widely-distributed economic growth; and for ensuring the diplomatic and military capacity to protect the expanding global presence and interests on which this growth depends.

Developments and trends in cyberspace play a key role across the spectrum of Scientific Development tenets, addressing automation and information needs for economic, political, public security and military progress; and providing means for information dominance in both domestic and international security arenas. This dominance corresponds to a general PRC strategic bent toward re-emerging as Asia's essential, or preeminent, actor on the road to mid-century objectives; it requires capabilities to both secure China's cyberspace capacity, and to hold at bay that of domestic and external competitors or adversaries.

Authoritative Chinese sources paint a cyber threat picture with three general components: hacking and cyber crime; Internet information management and propaganda; and military vulnerabilities. Concerning hacking and crime in cyberspace, Chinese media have published articles purporting that China is the "number one victim of cyber-attacks in the world." These articles largely define "hacking" and "cybercrime" as domestic and international law enforcement issues. Sources claim many attacks originate abroad, while others stress that bank fraud, gambling, and other cybercrimes are often perpetrated by domestic actors.

Chinese authorities have identified social media platforms where Chinese citizens are able to rapidly gain access and exchange information as the primary source of "misinformation, dissemination of rumors, popular discontent, chaos, political destabilization, and terror that can cause panic, lead to social crisis and turmoil, and overthrow the regime." Sources indicate that these threats emanate from both internal and external actors, and Chinese authorities continue to view efforts at Internet control and management as essential to protect the sovereignty and integrity of the Party and state.

In the military vulnerabilities arena, People's Liberation Army (PLA) leaders and strategists are keenly aware of the many military applications of information technology and systems networking, and have closely observed U.S. doctrine and practice in these areas. Most PLA writing and thinking about cyber threats is couched in the PLA doctrine of "informatization" and reflected in the PLA's task of preparing "to win local wars under informatized conditions." Many PLA writings view U.S. dominance in cyberspace as the key vulnerability of China's security and military systems.

Strategies to address domestic threats include Internet and social media control to address individual "rumor-mongers," "revisionist organizations," and separatists, while maintaining outlets for approved social discourse and propaganda. Regarding external threats, strategies focus on both defensive and offensive capabilities to counter advanced information operations by the United States, Japan, and other technically advanced actors. To enhance active cyberspace defense, China also has clearly developed cyberspace espionage and counter-intelligence tools to "shape the battlefield" at home and abroad. Among the organizations responsible for threat response and conflict preparation are the Ministries of Public Security, Industry and Information Technology, and State Security; the Propaganda Department; the Third and Fourth Departments of the PLA General Staff; PLA Technical Reconnaissance Bureaus; state-affiliated hackers; and a number of research institutes.

China's "active defense" strategy in cyberspace is characterized as focused on information dominance in modern conflict. PRC cyber capabilities are designed to enable a broad range of PLA command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) operations; the counter-C4ISR operations needed to achieve information dominance over an adversary; and advanced weapons system employment. In addition to serving as enablers or "combat multipliers," cyber operations also provide a distinct line of operations under a broader "integrated network electronic warfare" framework. The Third and Fourth Departments of the PLA General Staff likely are the key actors in the development of capabilities in this area; and evolving military strategy and doctrine for conducting information operations "campaigns" is a current focus on strategic discussion and debate. Issues of war control and deterrence in cyberspace also feature prominently in this debate.

Economic Drivers

Investigating the Chinese Underground Economy of Information Security

Zhuge Jianwei, Network Research Center, Tsinghua University, and CCERT Team, CERNET Network Center

Gu Lion, TrendMicro Company

Duan Haixin, Network Research Center, Tsinghua University, and CCERT Team, CERNET Network Center

In China, online business and entertainment has increased rapidly with the development of the Internet and its increasing number of "netizens." However, Chinese netizens are always suffering from a variety of security threats targeting their economic benefits, real or virtual. Behind those online threats is a complex underground criminal economy, supported by a variety of information techniques. Although a global issue, the underground economy of information security in China is unique in many aspects, because of the difference between Chinese economy, laws, and culture and those of Western countries. However, these issues have not received enough attention from the research community. Through measurement of the underground black markets, we were able to observe common advertisement and communication behaviors, and present detailed empirical analysis.

A structural analysis of the underground economy reveals the main profitable value chains and implementation techniques and identifies the phases and roles of different participants. The overall economy includes four value chains: 1) Real asset theft: stealing money from the stolen bank accounts or credit cards; 2) Network virtual asset theft: stealing virtual currency, equipment from stolen online game accounts, and selling them for real money; 3) Internet resources and services abuse: taking advantage of the snatched Internet resources including compromised hosts, hacked servers, and infected smart phones, to abuse the Internet services for profit; 4) Black hat techniques, tools, and training: selling Trojan horses and attack tools employed to provide technical support for the cybercriminals, and providing training services to newbies.

We present the first attempt at a detailed estimation on the overall damage of and population threatened by the underground economy, based on our structural analysis and investigation, and combined with reports from security vendors and government. We estimate that the overall damage to the Chinese economy exceeded 5.36 billion RMB ($USD 0.852 billion), affecting 110.8 million Chinese users (~22 percent) and 1.1 million websites (20 percent) in 2011.

Empirical analysis covers 8 years of data from the black markets built on Baidu Post Bar, the largest Chinese Web forum, and one-month data from black markets built on Tencent QQ chat groups. We show the increase of the black markets according to the amount of posts, threads, and participants, as well as their distribution and behavior. We also performed price analysis for the selected most popular goods and services in the black markets. Through this analysis, we can see the current situation and developing trends of the underground economy in China: the markets are growing rapidly in terms of the number of posts and of participants. In 2011, there were at least 90,000 participants involved in the measured black markets, who posted more than 320,000 messages belonging to 80,000 threads, which reflects the blooming situation of the underground economy in China. Our long-term empirical analysis of the dataset also reveals the structural and quantitative characteristic of the Chinese underground economy, including market behaviors, participant distribution, market business, and cheating behaviors.

We investigated the effectiveness of monitoring the black market to support the investigation of cybercrime cases, by a correlation analysis between the critical information of the cybercrime cases and the information in black markets. We select four typical public cybercrime cases and search in the dataset of black markets for some related unique information for attribution (such as a nickname or an online ID). The results show that the monitoring of underground black markets can support the earlier tracking and prevention of some ongoing cybercrime activities, and can also provide some critical information for case investigation. Therefore, for cybercrime emergency response teams and law enforcement agencies, continuous tracking and monitoring of the underground black markets has a very important practical significance. We suggest fighting against the underground economy by monitoring black markets and enhancing the cooperation between information security communities and law enforcement.

Information Security and the Dynamics of Innovation

Richard P. Suttmeier, Professor Emeritus, Department of Political Science,
University of Oregon

In exploring the relationships between innovation and cybersecurity in China, several issues can be identified. First, as is true with many other technologies, security concerns often serve as a driver of innovation. Conversely, new technological innovations often serve as drivers for new security concerns. Second, as is true in other countries, excessive attention to security, by limiting free flows of information and interchange, can limit innovation. Third, in light of the literature on the sociocultural “shaping” of innovation, an argument can be made that more attention be given to the existence of an “information culture” in China as an influence on the direction of innovation.

The interaction of concerns for innovation and concerns for security are evident in Chinese technology policy in a number of instances. In the case of the WAPI wireless standard, for instance, the ostensible reason for developing the standard was the perceived security weaknesses of the widely used IEEE 802.11. Clearly, however, the developers of the WAPI standard were also motivated by commercial interests. In the case of the Multi-level Protection Scheme, we see concerns regarding information security driving the promotion of the certification scheme, but these are again mixed with commercial interests and concerns for the development of innovative capabilities.

Information security concerns also figure prominently in the major national R&D programs of China more generally. Chinese distrust of the security provisions of the "Wintel" platform has motivated R&D efforts in both chip design and development and software. China's Medium to Long-Term Plan (MLP) for scientific and technological development, with its megaprojects, and the more recent Strategic Emerging Industries (SEI) initiative, have incentivized Chinese research establishments and industrial enterprises to develop their own intellectual property (IP), but their inability to do so in many cases has also incentivized these actors to acquire foreign technology that then can be slightly modified in order to secure Chinese IP rights. The growth of cyber industrial espionage may be one outgrowth of these policies and the incentives they provide. The heavy emphasis placed upon progress in ICT in the MLP and the SEI, and the stress on developing Chinese IP and Chinese technical standards for these technologies, is interwoven with security concerns and again calls attention to the issue of information culture.

While the existence of distinctive information cultures can be disputed, there are, nevertheless, suggestive differences in attitudes and values about information in different societies. This is especially true when we consider the default assumptions about information in society. In comparing China to the United States, for instance, one would find differences in attitudes with regard to ownership (public versus private, the value of IP rights, and understandings of the value of intangible assets more generally), to control (tight versus loose, the role of the state, the role of markets and civil society), and to sharing (circumstances under which information sharing leads to positive sum, negative sum, and zero-sum outcomes). These differences presumably are a function of some mix of the nature of political systems, the nature of the economy, and the level of economic development, as well as historical factors dealing with deeply-held values concerning risks and vulnerabilities.

Several implications for international cooperation on information and cybersecurity follow from these reflections. First, information security concerns are often mixed with economic and other considerations, making it difficult to identify a single interlocutor for discussions of cooperation. Second, if information culture is as salient as suggested above, successful efforts at international cooperation must begin with a more careful understanding of the attitudes and values towards information found in different societies. Finally, the relationships between innovation and security suggest that information and cyber security issues are not static, that they evolve with changes in technology, and that, therefore, there are significant opportunities for cooperative learning in working towards more cooperative solutions to information and cybersecurity dilemmas and conflicts.

Comparative Perspectives

The Economics of Information Security: Western Lessons for China?

Tyler Moore, Bobby B. Lyle School of Engineering, Southern Methodist University

Economics puts the challenges facing information security into perspective better than a purely technical approach does. Systems often fail because the organizations that defend them do not bear the full costs of failure. In order to solve the problems of growing vulnerability and increasing crime, solutions must coherently allocate responsibilities and liabilities so that the parties in a position to fix problems have an incentive to do so. This requires a technical comprehension of security threats, combined with an economic perspective to uncover the strategies employed by attackers and defenders.

In many circumstances online risks are allocated poorly. Perfect security is impossible, but even if it were, it would not be desirable. The trade-off between security and efficiency also implies that there exists an optimal level of insecurity, where the benefits of efficient operation outweigh any reductions in risk brought about by additional security measures. In the security space there is a dearth of relevant data needed to drive security investment. One reason why it is hard to come by good estimates of information security losses is that victims often have an incentive to under-report incidents. Unreliable information takes many forms, from security vendors overstating losses due to cybercrime to repeated warnings of digital Armageddon caused by the exploitation of process control system vulnerabilities while suppressing the discussion of realized or attempted attacks. The existence of an information asymmetry does not necessarily mean that society is not investing enough in security, nor that too much money is being allocated. Rather, it simply means that it is likely not investing in the right defenses to the ideal proportion. Furthermore, the IT industry is characterized by many different types of externalities, where individuals' actions have side effects on others: there are network externalities, externalities of insecurity, and interdependent security.

Each of these economic barriers is also likely to apply to Chinese firms and to China itself. There are some differences, however, which could serve as a basis for cross-country comparison. First, the incentives among stakeholders in China may be different. The information security industry is dominated by U.S. and European firms. Consequently, there may be a reduced potential for incentive conflict for China to advocate policies that might improve information security even when it threatens the business models of the security industry. For example, it has been demonstrated that security firms are quite reluctant to share data on security incidents and threats, even when doing so could substantially improve overall security. China may be willing to facilitate cooperation on sharing security information even in circumstances that the West refuses. Second, externalities may be viewed quite differently in China than in the West. Take industrial espionage. From the victim's perspective, losing trade secrets from infected computers is obviously negative. However, to the perpetrator, this is a benefit. Consequently, it is a more difficult calculation to decide whether the widespread vulnerability of the world's computers offers net benefits or harms. If, as is frequently alleged, China has adopted an industrial policy that encourages or at least tolerates conducting espionage on behalf of its own firms, then the gains to China must be weighed against the vulnerability of Chinese Internet users whose computers may become infected and cause harm.

In Western countries, it is apparent that policy interventions (safety regulations, software liability, indirect intermediary liability, public–private partnerships, information disclosure requirements, cyber insurance) will remain light-touch and hands-off because of policy deadlock and fear of harming Internet efficiency. Voluntary information disclosure and public–private partnerships are preferred, perhaps coupled with some safety regulation in critical infrastructure sectors. It is possible that China could choose to adopt variants of these approaches when constructing its own information security policies. However, there may also be opportunities to try interventions that are unlikely to gain traction in the West. For example, while software liability is a non-starter in most Western countries, it could conceivably be applied in China, which lacks a strong software industry. This could serve as a useful comparison to the more hands-off approaches tried in other countries.

In sum, economic analysis has turned out to be a very powerful tool for engineers and policmakers concerned with information security. Systems tend to fail when those who defend them are not the ones who suffer when they fail. An assortment of economic barriers, namely misaligned incentives, information asymmetries, and externalities, can cause problems for those who would protect information systems. However, a range of policy options are available to deal with the challenges, and some of the lighter-touch ones including information disclosure are being tried with some observable success. As China considers its own strategy for information security, it would be wise to learn the lessons already examined by researchers in this discipline.

National Strategies for Information Security and Industrial Performance

Danielle Kriz, Information Technology Industry Council

Cybersecurity is rightly a priority for governments globally, including those of the United States and China, as well as for information security firms. All companies want a secure digital infrastructure for commercial transactions, and to ensure the continued viability of the infrastructure and growth of their sector, technology companies are particularly motivated to design and build security into the DNA of their products and systems. Governments, respectively, desire a secure global digital infrastructure for economic growth, prosperity, efficiency, and protection. As industry and governments work together to develop the right policy framework to enhance cybersecurity, they should observe six guiding principles:

- Leverage public–private partnerships and build upon existing initiatives and resource commitments;
- Reflect the borderless, interconnected, and global nature of today’s cyber environment;
- Be able to adapt rapidly to emerging threats, technologies, and business models;

- Be based on effective risk management;
- Focus on raising public awareness; and
- More directly focus on bad actors and their threats.

Unfortunately, governments sometimes react to cybersecurity concerns without fully considering the global context or consequences of their policy proposals. Some cybersecurity-related laws, regulations, and other requirements are enacted in the name of supporting national security interests but might ultimately decrease security and disrupt global commerce. For example, there are cases when vendors of security products must disclose key intellectual property to enter the market or to use domestic security standards in products sold in that country. There also exist some outright bans on the sale or use of imported or foreign encryption products or the sale of certain IT products for unsubstantiated security reasons. Unique, country-specific security standards and other requirements can undermine security, raise costs, slow innovation, impede interoperability, and fragment the Internet. Some of these practices are promoted with limited transparency or engagement of the private sector.

In the United States, both Congress and the Administration have made a growing number of policy proposals over the past 6–12 months related to cybersecurity. In Congress, a variety of legislative proposals have come out of the Senate and House. Despite intense debate, none of these proposals have passed or become law—and they might not, given the increasingly partisan tone around cybersecurity and legislative gridlock in an election year. While the technology industry almost unanimously supports Congressional action on discrete topics that will demonstratively improve cybersecurity—information sharing on cyber threats, reform of the Federal Information Security Management Act (FISMA), cybersecurity research and development (R&D), enhanced penalties for cybercrime, and a national data breach standard—the industry has a less cohesive outlook on proposals to give the Department of Homeland Security additional power related to cybersecurity, or proposals to regulate cybersecurity in critical infrastructure. Industry's concerns revolve around fear of an over regulatory approach that is U.S.–centric, would balkanize cyberspace, and would decrease security.

In the U.S. Administration, various departments and agencies have some responsibility related to cybersecurity, including the White House, Department of Homeland Security, Department of Defense, Department of Commerce, Department of State, National Institute of Standards and Technology (NIST), and others. Some of them are considering new policies and programs to augment their current domains. The technology industry supports some of these, such as the Commerce Department promoting voluntary cybersecurity efforts in industry and the Office of Science and Technology Policy's national strategy for cybersecurity R&D. However, Defense Department proposals to regulate the technology supply chain create a great deal of concern. Not only will this likely decrease security, but it will harm innovation and send the wrong signal to U.S. trading partners regarding the government's role in private-sector business decisions related to product security. In fact, the Information Technology Industry Council already is concerned about new supply chain management provisions in the 2011 National Defense Authorization Act (NDAA, Section 806) and the 2012 Intelligence Authorization Act (Section 310).

China has also proposed or enacted cyber-related policies that are over-regulatory. The 1999 encryption regulations restrict or ban outright the use of foreign encryption technology. Under the China Compulsory Certification for Information Security ("CCCi"), 13 technology product categories must undergo stringent certification procedures for sale in China, albeit only for government procurement. In the Multi-Level Protection Scheme (MLPS), information security products sold into information systems ranked "3" or above must include Chinese indigenous IP, and for products sold into all systems levels a vast array of underlying standards mandates arduous product functionalities.

Taken together, these policies can or could significantly reduce the universe of available technology within our markets. This ultimately will impede the ability of our countries' governments and businesses to adapt to new, borderless cyber threats or online crime, fraud, and theft. It will also slow domestic innovation. Given that security underpins the use of the Internet and e-commerce, the ultimate result is slowed economic development worldwide.

The technology industry urges both governments to pursue cybersecurity policies in a manner that will achieve the requisite levels of security needed to meet national security concerns while preserving interoperability, openness, and a global market. In fact, such an approach results in better security. In the right policy environment, we can increase security while maintaining cyberspace's overall benefits.

Economic and Legal Challenges in American Cybersecurity

Fred H. Cate, Distinguished Professor and C. Ben Dutton Professor of Law,
Indiana University Maurer School of Law

U.S. government officials purport to acknowledge that cybersecurity is a very important issue, as can be seen in statements such as the final report of the president's 60-day cybersecurity review and the 2010 quadrennial intelligence review of terrorist threats facing the United States. However, officials are not very precise when talking about cybersecurity. This was evident, for example, in President Obama's May 29, 2009, East Wing press statement on cybersecurity, where he identified as "digital infrastructure" risks: "cyber thieves trolling for sensitive information," "the disgruntled employee on the inside," "the lone hacker a thousand miles away," "organized crime," "the industrial spy," "foreign intelligence services," "cybercrime," (by which I think he meant identity theft), "hackers gain[ing] access to emails and . . . campaign files," "stealing money from ATM networks," cyber intruders . . . prob[ing] our electrical grid and in other countries . . . plung[ing] entire cities into darkness," "constant attack[s] . . . [against] our defense and military networks," "Al Qaeda and other terrorist groups . . . [threatening to] unleash a cyber attack on our country—a weapon of mass disruption," "malicious software—malware," "a glimpse of the future of war," and "Mumbai terrorists rel[ying] not only on guns and grenades but also on GPS on phones using voice-over-the-Internet." We have almost no data about the prevalence or impact of these threats, which when combined with such broad and vague definitions makes it almost impossible to formulate rational policy or measure their effectiveness.

There are complicated organizational and cultural issues within the U.S. government. The president rejected demands that he appoint a cybersecurity "czar," with real authority over at least government computer systems. Instead, he opted to appoint a cybersecurity "coordinator," with almost no authority and a limited budget. Even that position took seven months to fill, reportedly because many of the candidates interviewed were concerned about the chance of succeeding in such a weak position. After all, frustration about lack of authority or resources has led almost every official to hold the U.S. cybersecurity portfolio since 9/11 to resign.

Cybersecurity is a field in desperate need for better incentives. At present it suffers from a "tragedy of the commons" phenomenon by which many key players assume someone else is providing for security, combined with a sense of despair about the size and complexity of the challenge that often frustrates significant investment. It is almost always preferable to allow markets to create appropriate incentives for desired behaviors, but there are occasions where government intervention is necessary. Information security is one of those instances. The threats are too broad, the actors too numerous, the knowledge levels too unequal, the risks too easy to avoid internalizing, the free-rider problem too prevalent, and the stakes too great to believe that markets alone will be adequate to create the right incentives or outcomes. Incentives can take many forms. The big challenges is to target the incentives well, not over-regulate, not mis-regulate, and not penalize those who are trying and may, on occasion, fail.

Cyber threats are especially serious because of our vast cyberinfrastructure. The past decade has been marked by a movement from secure proprietary networks (or from no networks at all) for critical infrastructure control systems, to a growing reliance on the Internet even by critical systems. ATM networks now use the commodity Internet. So do credit card transactions. Control systems for airplanes, trains, and natural gas pipelines all use the Internet, sometimes with wireless switches. We are moving to a smart grid for electricity—controlled by the Internet. Just-in-time supply chains are increasingly common and all rely on the Internet. These technologies increasingly dominate every aspect of our lives. They almost all connect via the Internet—and therefore are susceptible to attack—and they all generate and store information about us that is also vulnerable to attack or misuse. The stakes are vast and our approach to cybersecurity is completely inconsistent.

Law is increasingly vital to provide appropriate incentives, create meaningful oversight, and protect individual rights that are often implicated by security measures. Yet, to date, the U.S. administration has largely overlooked—or even taken off the table—the role of law. Moreover, the law today surrounding privacy—of which security is a key component—is a mess. Modern privacy law is hopelessly outdated. Courts have described privacy law as “caught up in a ‘fog,’ ‘convoluted,’ ‘fraught with trip wires,’ and ‘confusing and uncertain.’”

Finally, there seems to be a growing amount of nationalism around information, which is ironic since data flows are inherently global. The United States targets China and Russia on cybersecurity issues. Europe and Canadian provinces target the United States on privacy issues. China, India, the United States, and other countries focus on the national origin of critical components of cyberinfrastructure in an effort to better secure that infrastructure. This petty nationalism does not enhance security or privacy. In fact, nationalistic responses diminish cybersecurity, as criminals operate freely across national borders that restrain our laws and enforcement.

Information Warfare Doctrine

Chinese Information War: Historical Analogies and Conceptual Debates

Jacqueline N. Deal, Foreign Policy Research Institute and Long Range Strategy Group

Information war in China, as elsewhere, is a large subject, encompassing many dimensions of activity. This discussion focuses on the particular question of Chinese information war in the context of a high-intensity conflict, and frames this question with reference to the historical analogies that Chinese military writers draw when discussing information war in high-intensity conflict. Chinese and foreign analogies arise in such discussions, so both are treated here. The intent is to try to understand which historical examples are cited, how they are interpreted, and what this might imply about Chinese conduct in a future conflict.

An American reader will likely say the discussion of information war is in fact a discussion of kinetic warfare (involving physical violence) in general—that is, we seem to address *warfare*, as opposed to *information*. This is because Americans tend to think of hacking and episodes like the Stuxnet attack on Iran when they hear the term information warfare. But Chinese strategists take seriously the idea that an information technology (IT) “revolution in military affairs” (RMA) characterizes the current security environment. “Warfare under informatized conditions” is the current Chinese guidance for the kinds of conflicts that the People’s Liberation Army (PLA) should expect to fight. Information war, therefore, is inseparable from Chinese thinking on future kinetic, high-intensity conflict in general.

Why focus on Chinese historical analogies for understanding information war? Driven by new technologies, new uses for existing technologies, and new forms of organization to exploit these technologies and applications, information war is rife with uncertainty. In the face of uncertainty about the future, all human beings fall back on familiar examples from the past. The Chinese may be particularly inclined to study lessons from historical cases for several reasons. First, China possesses a rich body of classical strategic literature that has been enjoying a renaissance within the PLA since Deng Xiaoping initiated the period of modernization in the 1980s. Second, this body of classical texts emphasizes the role of information in warfare. In fact, the Chinese corpus puts information—superior intelligence—at the center of warfare and strategy in a way that distinguishes it from canonical Western works such as Clausewitz's *On War*. Finally, the PLA has not fought a high-intensity conflict since the 1979 Sino-Vietnamese War. Although that conflict persisted into the 1980s, today's PLA suffers from a dearth of recent experience of its own to inform its doctrine and training. This compels turning both to Chinese lessons from the past and to the contemporary experience of other militaries.

The secondary literature on Chinese information war features three key debates that this paper aims to illuminate. First is the debate over whether current Chinese thinking reflects primarily U.S. or Russian influence. James Mulvenon and Toshi Yoshihara have both pointed out the apparent mimicry of U.S. writings in Chinese military texts on information war. Tim Thomas has noted that the same writer appears to be channeling Russian writings in one article and American writings in another.

The second key debate concerns whether Chinese information war applies primarily in peacetime, war, or both? Edward Sobiesk has argued that China is today engaged in a long-term peacetime information war effort that is "not about fighting," per se. But this argument seems at odds with the emphasis on preemption and active defense in official Chinese defense texts, as noted by other secondary sources.

A final debate revolves around the influence of classical Chinese strategy and whether China has a distinctive approach to information war. Kate Farris notes that while the United States initially identified six pillars of information operations in a 1998 Joint Doctrine publication—psychological operations (psyops), denial and deception (D&D), electronic warfare, computer network attack (CNA), physical destruction, and operational security—U.S. efforts seem to have focused almost exclusively on the CNA pillar. China, by contrast, seems to be most concerned with the psyop and D&D pillars. Thomas has classified the Russians and Americans as being on opposite ends of a spectrum from most valuing to least valuing information war. He locates the Chinese as being at an intermediate position on this spectrum.

With regard to these three debates, while both U.S. and Russian influences are present, the Chinese approach to information war may be closer to the historical Russian approach. Similarly, Chinese information war efforts in peacetime should not be viewed as independent, isolated efforts. Rather, they are necessary for and designed to facilitate potential Chinese actions in a kinetic, high-intensity war. Finally, classical Chinese strategic thought does shape China's approach to information war. Consistent with the lessons of Sun Zi and other ancient Chinese thinkers, contemporary PLA strategists assign critical importance to the intelligence preparation of the battlefield, to facilitate a rapid Chinese victory at a minimum cost. Information war lies at the heart of this effort, as it should enable Chinese forces to disable the enemy's most important but also most vulnerable systems at the outset of a conflict and thus convince the adversary to capitulate.

Many Chinese authors diagnose the IT RMA—even if they don't call it that—as a major shift in the character of warfare. In the latter part of the Cold War, while the United States focused on the precision strike component of the RMA, the Russians developed complementary concepts of Radio-electronic Warfare along with their ideas about emerging Reconnaissance Strike Complexes. Like the Russians, the Chinese seem to be developing an approach that integrates cyber war and precision strike, along with other kinetic and non-kinetic means, in their version of the IT RMA. Warfare in the age of the IT RMA, according to contemporary Chinese authors, blurs the lines between offense and defense, and demands action in multiple dimensions of space to produce timely attacks on adversary sensors and neutralize adversary strike assets. The Chinese often identify inducing desirable psychological effects as the goal (e.g., paralyzing the enemy).

However, given persistent challenges in the area of human capital, there are real questions about how the PLA will integrate and structure the use of the capabilities required to execute the operations described in Chinese writings on warfare under informatized conditions. For instance, will the Chinese opt for delegation of control over key assets and capabilities to relatively low-ranking operators, maximizing flexibility? Or will a Chinese preference for centralization lead to an emphasis on well-rehearsed sequences of action that depend on the accuracy of intelligence collected in peacetime, which might reduce the PLA's ability to respond nimbly to changing facts on the ground? To the extent that well-rehearsed sequences of action are important, will the PLA create a credible Blue exercise force, increasing the chance of Red failures? In general, how will Chinese brass manage the tension between the Chinese penchant for secrecy and the need to train forces in the use of techniques suited for warfare under informatized conditions? (How much information about Red's vulnerabilities will be shared with Chinese Blue teams for the purpose of exercises?)

These questions for future research tend to involve issues of organizational culture, at least some of which can be investigated through open-source writings. Overall, the research suggests that information war is critical to Chinese thinking on future war in general. American defense planners may therefore want to widen the aperture on studies of information war to include not only peacetime concerns with intellectual property theft and viruses but also potential military applications of capabilities gained through espionage and knowledge of the vulnerability of key surveillance, command and control, and strike systems.

Comparing Chinese and Russian Approaches to Information Warfare

Timothy Thomas, U.S. Army Foreign Military Studies Office

All cyber activities are not alike. They depend on the context and culture of the side engaged in the issues. For example, some Chinese advocate using packets of electrons as stratagems to conduct cyber reconnaissance or attacks. A stratagem is designed to mislead enemy processes of perception, thinking, emotion, and will. In this case, packets of electrons could be used to fulfill stratagems such as "rustle the grass to startle the snake" (throw thousands of pings at a site until it becomes clear where firewalls pop up). Russians don't think in this way but rather use the term asymmetric warfare to describe offset or indirect tactics they might use.

Many Chinese cyber concepts differ either in meaning or content or both from Russian concepts. Some cyber-related terms in the Chinese vocabulary include water army, 50 cent party, human flesh engine, system sabotage, integrated network electronic warfare, *shi*, cocktail warfare, and war engineering. China stresses its soft power approach more than Russia. In a 2005 article in *China Military Science*, author Wang Shudao noted that China must take action "to propel China's culture industry and media industry beyond China's borders in an effort to take over the international culture market." Today China is taking out full page ads periodically in the *New York Times* and *Wall Street Journal*.

China is likely influenced by the tactics known as "cocktail warfare," a concept developed in the 1999 book *Unrestricted Warfare*. One of the book's authors, Qiao Liang (a colonel at the time), wrote that new concepts of weapons involve the ability to combine various elements to produce types of weaponry never imagined before. For example, Qiao may be referring to combinations such as "cyber preemption + network reconnaissance + high-technology deception + financial market disruption + network deterrence" to produce an overall effect and a new weapon.

Russia's Ministry of Defense in 2011 proposed "Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space," something the PLA hasn't done in open source. The Conceptual Views document defined terms that included, as in 1995, information warfare and information weapons, among others. Conceptual Views also offered principles (legality, priority, integration, interaction, cooperation, and innovation) to guide the activities of the Armed Forces of the Russian Federation in information space. The Conceptual View further included rules for the use of information space (as an agent of conflict deterrence, conflict prevention, and conflict resolution).

Russia's cyber lexicon is closer to that of the United States. They define terms such as cyberspace, cyber attacks, cyber war, and others. Cyberspace is viewed as an objective reality, a medium for computer functions in which one can affect an enemy's systems and protect one's own. A cyber attack was defined as a form of hostile actions in cyberspace aimed at cyber systems, information resources, or an information infrastructure to achieve some goal, implemented with special programs, equipment, and methods. Cyber war was defined as the systematic struggle in the cyber domain among states, political groups, and extremist and terrorist groups, where targets are information resources and whose properties (integrity, accessibility, and confidentiality) can be violated.

Both Russian and China seem to favor the use of the term control to a much greater extent than the United States. This difference is often reflected in internal debates and the need to restrict freedom on the web. Another common point is that both nations have developed long-term cyber plans. For China it is the Informatization Development Strategy and for Russia it is the Doctrine of Information Security.

Similarities in the Chinese and Russian approaches are that both countries are signatories to the recently proposed Internet Code of Conduct; both countries worry about cyber's influence on the public's cognitive aspect; both countries are working on GPS systems, Beidou in China and Glonass in Russia; both countries have begun a focused development of new concept weapons as a source of asymmetrical counter weapons, to include electromagnetic pulse, rail guns, nano-technology development, and so on; and both countries rely heavily on Marxist thought. Differences include the fact that Russia is in a soft power protection mode while China is involved in both domestic protection and foreign exploitation for intelligence. Russia does not seem to have as many clarifying cyber terms (water army, human flesh engine, etc.) as the Chinese; and China seems to have not developed a concept to date for its military as the Russians have done with their "Conceptual View" document.

Military Organizations

People's Liberation Army Infrastructure for Cyber Reconnaissance

Mark Stokes, Project 2049

Nestled in the quaint Xianghongxi community in the western hills of Beijing's Haidian District, the PLA General Staff Department (GSD) Third Department manages a vast communications intercept infrastructure targeting foreign diplomatic communications, military activity, economic entities, public education institutions, and individuals of interest. GSD Third Department may serve as national executive authority for computer network exploitation (e.g., cyber reconnaissance).

This hypothesis is based on three assumptions. First is the gradual technical and organizational integration of signals intelligence, information security, and cyber reconnaissance. Second, the Third Department's core competency is in advanced computing and cryptology. Computing and cryptology are central to computer network operations (CNO). Finally, the Third Department serves as China's largest employer of well-trained linguists for translation of collected information. GSD Third Department may be supported by commercial enterprises and universities.

The Third Department Director reports to the Central Military Commission (CMC) through the Chief of General Staff. A preliminary hypothesis is that a key Chinese Communist Party (CCP) or State Council leading group coordinates general policies on information security and computer network operations. Priority may be granted to defense against perceived security threats to the CCP. The Third Department likely plays a central role in civilian information security organizations, along with internal security entities such as Ministry of State Security (MSS) and Ministry of Public Security.

The GSD Third Department is separate and distinct from Military Region and Service-level technical reconnaissance bureaus (TRBs). TRBs likely enjoy significant operational autonomy, possibly including cyber reconnaissance operations. As such, relatively independent TRBs could limit power of Third Department, create natural bureaucratic competitions, encourage "stove-piping" of technical and policy programs, and limit overall efficiency and effectiveness. Cyber espionage directed against international organizations could benefit from technology development funded under the 863-917 Program.

The organization responsible for computer network attack (CNA) mission remains unknown. Candidates include the GSD Fourth Department and Second Artillery Force. Among all PLA service branches, the Second Artillery may best understand nodal analysis and the art of strategic targeting. GSD Fourth Department's core competency is operational-level electronic countermeasures. The department's leadership may have lobbied for the strategic CNA mission several years ago.

Understanding of China's cyber operations capabilities could benefit from more in-depth research. For example, a better grasp of Third Department/TRB organization, history, and missions are needed. Greater research could be directed toward China's domestic information security challenges and national computer network defense organizations and relationships. A better understanding of Third Department R&D institutes and relationships with defense industry is warranted as well. More details on Third Department relationships with small- and medium-size information security/IT enterprises could be of significant value, as could more information on "cyber militia," its role in computer network operations, and command and control relationships.

An examination of opportunities and obstacles in development of international cyber "rules of the road" would be worthwhile as well. Better understanding is also needed of the role of SIGINT/cyber reconnaissance in "informatized" warfare, including cueing support for long-range precision strike operations and the ASBM. Finally, a deeper knowledge of the organization and CNO missions of the GSD Fourth Department and Second Artillery may be worth considering.

Civil–Military Integration and China's Cyberspace Operations: Investigating PLA Cyber Militias

Robert Sheldon, US–China Economic and Security Review Commission

Steve Glinert, Defense Group, Inc.

We assess Chinese civil–military integration (CMI) in the context of cyberspace operations. Specifically, we evaluate People's Liberation Army (PLA) "cyber militias" as a case study in the ostensible appropriation of civilian talent for military ends. To research this issue, we identified a sample of 64 cyber militias referenced in Chinese-language resources. On the basis of this dataset and related materials, we analyze cyber militias' peacetime and wartime functions, roles, and missions, their associations and command and control relationships, the rate of creation, geographic dispersion, and other associated issues.

We argue that cyber militias do not represent the “pointy end” of China’s cyber spear, but nevertheless merit consideration. Although much remains unknown about cyber militias’ functions, we assert that their responsibilities tend toward defensive rather than offensive operations, notwithstanding contrary claims made in enthusiast literature and popular media (in both China and abroad). We did not identify compelling evidence to suggest that cyber militias routinely conduct peacetime intelligence operations. Their frequent collocation with Ministry of Science and Technology (MOST) “high-tech development zones” is an interesting finding that is perhaps symptomatic of a reference to high-tech militia development within one or more of China’s major national-level development plans (or perhaps just within local implementation guidance). Finally, foreign businesses and educational institutions interact with organizations that host cyber militias, which we characterize as potentially problematic.

There are several issues raised in our paper that require further examination, including: the incentives or mandates that lead to the creation of new cyber militia units; the nature and extent of connections between cyber militias and MOST high-tech development zones; cyber militia organizational features and PLA affiliations; and cyber militia-PLA joint training activities. Further research could include: more systematic collection of cyber militia data; more rigorous application of quantitative methods for analyzing our dataset; closer examination of one or two cyber militias, including identification of specific members, for better insight into their functions; field work, including interviewing cyber militia members and/or host organizations; and consideration of CMI-related writings that focus more on China’s national defense mobilization system (as opposed to materiel-related CMI writings).

Perhaps the most striking feature of our discussions was the diversity and range of presentations delivered. This helped to underscore the broad scope of the China/cybersecurity challenge. Also fascinating was that, in 2012—over 10 years since the earliest examples of Chinese computer network exploitation and computer network attack—many fundamental questions about China’s cyber activities remain.

Intelligence Issues

Chinese Intelligence Operations and Transnational Consequences

Nigel Inkster, International Institute for Strategic Studies

China’s intelligence services have been in their current form since the early 1980s: the Ministry of State Security whose priority is dealing with threats to internal stability including the “three evils” of separatism, terrorism, and religious extremism, but which also collects foreign intelligence; and the Second and Third Departments of the PLA General Staff dealing respectively with military and foreign collection and signals intelligence (SIGINT).The PRC has no central coordination or oversight structures for intelligence nor is there any central intelligence assessment mechanism. The top-level interface between intelligence and policymaking is through the mechanism of a variety of Leading Small Groups, some better established than others and whose effectiveness is determined by their composition and chairmanship.

China's intelligence services work differently from their Western and Russian counterparts. Virtually no covert collection takes place through legal residencies and the Chinese government seldom if ever comments publicly on intelligence operations directed against it or on Chinese operations which have been compromised. Until well into the 1990s, Chinese foreign intelligence operations relied almost exclusively on the use of agents within Chinese diaspora communities, particularly those employed in the U.S. high-tech or defense industry sectors, although they have latterly shown greater confidence in approaching non-Chinese targets. Since 1986 a major imperative of Chinese foreign intelligence collection has been the 863 Program, designed to enable China to catch up with the West in key strategic industries. The 863 Program was initially focused on enhancing China's military capabilities and responsibility for collection against the program was not limited to China's intelligence organizations; employees of state corporations, academics, and students also played a role. In 2004 President Hu Jintao's New Historic Missions of the Armed Forces in the New Period of the New Century expanded the PLA's national security role to encompass the preservation of the Communist Party and the promotion of China's economic development, with potential implications for their collection role.

The way in which cyber espionage is conducted within China remains opaque, but such evidence as there is points to an evolution from an initial "Wild East" approach involving numerous actors with varying degrees of state connectivity towards something more obviously centrally directed from an operational perspective, although there is no evidence of any structured policy oversight for this activity. Operationally 3/PLA is in the driving seat: almost all serious exploitation operations are directed out of 3/PLA official premises. The focus has increasingly been on penetrating core systems—e-mail and social networking services and those offering access to encryption systems and source code—to provide the widest possible primary database which can enable more precise targeting of specific systems.

The focus of Chinese cyber espionage includes the following: 1) the three evils as exemplified by the attacks on Tibetan exile computer systems described in the Citizen Lab's GhostNet investigation. The GhostNet investigation revealed a huge range of infected computers, many of which belonged to foreign governments and NGOs; 2) U.S. and other Western high-tech weapons systems; 3) U.S. and other Western intellectual property in areas of strategic concern to China; and 4) details of negotiating positions of Western firms competing with Chinese companies for contracts overseas.

The Chinese Communist Party's continued hold on power is seen as depending on the neutralization of sources of dissent and the maintenance of high levels of economic growth. China has still to lift another 400 million people out of poverty and continue a program of large-scale urbanization but also faces the additional challenge of avoiding a middle-income trap. China thus has an existential imperative to develop a world-class corporate sector able to compete with existing multinational corporations. Meanwhile, as China's overseas interests have grown, the leadership is under growing pressure to defend those interests in a more assertive manner. Cyber espionage offers China an asymmetric advantage which it can be expected to exploit to the full with little concern for the reputational impact of such behavior.

For China's intelligence services and for the country generally, the capacity to undertake large-scale cyber exploitation operations represents a step-change in capabilities. It eliminates much of the risk associated with traditional collection techniques, provides much greater reach, and has massively increased the quantities of information which can be collected. It remains to be seen what practical advantage China will be able to derive from the information it collects or how great its ambitions will be in terms of using cyber collection as an adjunct to more aggressive human intelligence (HUMINT) operations. It is clear that this is already happening in relation to MSS work against the "three evils" and it is possible that Western groups and even governments seen as supportive of dissident Chinese organizations can also expect to be targeted; but there is so far no sign of this translating into a more aggressive approach to HUMINT operations against other target areas on the back of cyber collection.

China can be expected to become more proactive in shaping the global cyber environment both in regard to promoting Chinese alternatives to Western hardware and software but also in areas such as Internet governance where, up until now, China has been content to follow in Russia's wake. In particular, China can be expected to influence "G77" states in favor of international positions that accord with Chinese objectives in areas such as information security.

So far the West has been unable to develop effective counter-strategies to this unprecedented, industrial-scale cyber exploitation. This reflects the difficulties Western governments have in coordinating responses with a private sector that has very different business drivers and perceptions of risk. In-domain response (countering cyber risks with cyber means) is difficult, not least because of a basic asymmetry of collection requirements and levels of vulnerability. Cross-domain responses (countering cyber risks with other policy or military instruments) and the threat of escalation could prove more effective, but a coherent strategy is proving elusive.

Escalating Cybersecurity Threats Pose New Energy Challenges for the United States

Melanie Hart, Center for American Progress

Academic research and policy discussions on cybersecurity traditionally focused primarily on the military domain. Much less attention has been paid to U.S.–China cyber tensions in the economic sphere, but that is changing rapidly. Chinese actors appear to be using cyberspace not only to infiltrate the U.S. military but also to pilfer trade secrets from private enterprises and to penetrate U.S. electric utility networks. These two types of cyber activities—economic espionage and critical network infrastructure (CNI) attacks—pose a growing threat to U.S. economic competitiveness, particularly in the energy sector.

The first threat—espionage and intellectual property (IP) theft—poses a direct and growing risk to U.S. clean energy competitiveness. China has an indigenous innovation program that aims to move the country up the value chain from lower-end manufacturing to higher-end technology innovation through a combination of long- and short-term industrial planning. The short-term policies are of particular concern because those policies encourage local officials to use WTO-illegal trade practices, forced technology transfer, and, in some cases, outright IP theft to reduce Chinese dependence on Western technology.

Those efforts focus particularly on clean energy because Chinese leaders view clean energy as the only critical strategic emerging industry where the United States does not already have an insurmountable lead. Conventional technology espionage is already a major problem in clean energy sectors such as wind and solar. Now these activities are moving into cyberspace, where the risks are much lower on the Chinese side (since cyber spies are harder to catch and prosecute than the traditional variety) and where the costs could be much higher for the U.S. companies targeted in these attacks (since cyber hackers can exfiltrate large volumes of information unbeknownst to the companies involved).

The second threat—critical network infrastructure attacks—poses both direct national security risks and indirect risks to our economic competitiveness. Electric utility networks utilize centralized industrial control systems (also called Supervisory Control and Data Acquisition, or SCADA systems) that were not designed for the Internet age but are increasingly going online. Those systems do not have robust network security, and as a result they provide cyber criminals a gateway for accessing and potentially bringing down critical utility networks. U.S. intelligence officials claim that Russian and Chinese hackers are already hacking into U.S. electricity networks and inserting malware that they could later activate (i.e., in a future conflict with the United States) to shut down the electric grid.

These network threats are serious, and more work is needed to improve security. The best path forward is to upgrade our utility grids to more modern ‘smart’ utility systems that can not only address current cybersecurity vulnerabilities but also facilitate our transition toward a clean energy economy. Unfortunately, there is a very high risk that we will do the opposite. Instead of using current network vulnerabilities as an incentive to make needed upgrades, many U.S. national security experts are calling for a halt in U.S. smart grid infrastructure roll-out. Those experts argue that since next-generation utility grids have more Internet-connected communication nodes, the expansion of nodes will by definition expand their vulnerability to attacks. Halting U.S. energy modernization is not the best path forward, however. The Internet itself also brought new cyber risks, but the efficiency gains made those risks worthwhile. The same applies for our utility systems, particularly since China and many other countries are moving quickly to modernize their own electricity networks. If the United States allows cyber concerns to halt economic modernization, that will erode our economic competitiveness and cede this battle to our attackers before we even begin.

More work is needed to lay a solid empirical groundwork for effective policy solutions to these new and growing problems. We need more information on cyber espionage and associated IP damages to the U.S. energy economy. At present, the United States does not have common accounting standards for measuring the damage from cyber intrusions and IP theft. We also lack mandatory reporting requirements to ensure that companies share this information. Both general accounting standard and mandatory reporting requirements will be necessary to create valid damage measurements, and those measurements are a critical first step in building political support for cybersecurity policy in Washington.

We need new models for prosecuting cyber espionage. The cyber domain adds another layer of confusion to what is already a difficult bilateral trade issue: figuring out how to prove and prosecute Chinese IP theft. Attribution is a major problem in the cyber domain. It is often very difficult, particularly in a legal sense, to prove who carried out a specific attack. Trade institutions for non-market economies may offer good models for cyber espionage attribution. Trade institutions utilize approximations (such as antidumping calculations) to get around policy transparency problems in non-market economies. Similar measurement approximations may be needed to prosecute IP issues in the cyber domain.

We need better administrative models for coordinating private sector responses to network infrastructure threats. The U.S. electric utility industry is highly decentralized. At present, no single federal regulatory has authority over our entire national utility network—most of the regulatory authority is at the state level. From a security perspective, that creates a major problem, because the state and local utilities do not exchange information on cyber threats or share common security standards. This decentralized system is an administrative barrier that many other countries do not face. While the United States has over 3,000 utility companies, China, for example, has only two, and that likely will make network security much easier to coordinate.

State and Society

The Human Rights Underpinnings of Cybersecurity

Sarah A. McKune, Citizen Lab, Munk School of Global Affairs, University of Toronto

When different perspectives and disciplines overlap, critical new questions and observations emerge in that space. The broad context of cybersecurity is informed by China's long-term military development and defense strategy, political economy factors, and the Chinese government's paramount interest in maintaining internal security through domestic control—often at the expense of human rights. It is thought-provoking to examine the link between cybersecurity and human rights from such angles.

When it comes to cyber, China's complex, multilayered policies and practices may best be described as fluid. Traditional military and Party doctrine operates alongside more recent imperatives of cyber defense and offense, while cyber espionage (information acquisition) against governments, corporations, and civil society appears to have become a core element of China's occupation of cyberspace. Regime stability is preserved through Internet censorship and online information control, with government organs and private companies together aggressively managing the flow of information to and among the public.

Yet at the same time, the picture that has emerged thus far of the structure and practices employed by the Chinese government to maintain control and advance its interests in cyberspace remains murky. The question of control itself requires greater research and empirical evidence. A variety of actors within China play a part in the cybersecurity equation, and the discrete roles of particular authorities and individuals, including privateers, cannot be overlooked. Methods of interaction between government organs on cyber issues merits further consideration. Crucial details concerning cyber threats (such as targeted malware attacks) linked to China are still outstanding, including key entities involved, the probable division of labor between government and private actors, and how such cyber campaigns are managed.

Citizen Lab has endeavored to produce concrete data regarding aspects of these issues through its long-standing research on targeted threats against civil society organizations. We have documented Internet censorship,[1] cyber espionage networks,[2] and targeted malware attacks[3] from a civil society perspective. Our research indicates that today's cyber threats in the civil society sector and beyond incorporate not simply techniques that are defensive in nature (such as Internet filtering), but highly offensive and strategic attacks, relying on what appears to be extensive surveillance and information gathering. Many attacks are politically motivated, as evidenced by: long-term campaigns to compromise specific actors working on human rights issues; the social engineering and timing of attacks, often linked to political developments; and the operation of the malware itself, which masks its presence and exfiltrates sensitive information over periods of time. Such attacks are highly adaptable, both to new media and to circumstances unique to particular organizations. Threats range from simplistic malware delivered through exceptionally tailored social engineering techniques, to uniquely-timed DDoS attacks, to Twitter "floods" against political hash tags. More research and collaboration in this field is essential to building

[1] The OpenNet Initiative, a collaborative partnership between the Citizen Lab, the Berkman Center for Internet & Society at Harvard University, and the SecDev Group, has documented Internet censorship and surveillance globally; its findings are available at http://opennet.net/.

[2] See Information Warfare Monitor and Shadowserver Foundation, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, April 2010, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0; Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, March 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[3] See Citizen Lab, "Information Operations and Tibetan Rights in the Wake of Self-Immolations: Part I," March 9, 2012, http://citizenlab.org/2012/03/information-operations-and-tibetan-rights-in-the-wake-of-selfimmolations-part-i/.

our understanding of the Chinese government's role in these cyber threats—a difficult issue given the limits of attribution based on technical forensics—and its overall cybersecurity agenda.

Additionally, Citizen Lab has focused on the cyber governance and political economy dimensions of China's cybersecurity efforts. The Chinese government has sought to preserve stability at all costs, especially post-Arab Spring, in this year of leadership transition; and in the view of the regime, civil and political rights, and the use of the Internet and ICTs to advance them, are a primary threat to this stability. The government has pushed in international fora—with varying degrees of success—for development of cyber norms that preserve its ability to manage cyberspace as an internal affair, and restrict freedom of expression when that expression includes dissent. Additionally, with China's own censorship infrastructure largely in order, the country has gone on to develop into a provider of filtration and surveillance technologies abroad. Chinese companies such as ZTE are among the key suppliers of filtration and monitoring technology to other authoritarian regimes, including Iran and the Gadhafi regime formerly in power in Libya. In sum, the Chinese government is in the practice of compounding its regime pathologies in the cyber context domestically, and exporting those abroad to the detriment of human and international security.

In examining the circumstances of cyber threats, particularly those faced by civil society, it has become increasingly clear that the policies and practices of the Chinese government concerning human rights have had a negative impact on cybersecurity. Long-standing human rights problems are playing out in the cyber realm, and constitute a major catalyst for cyber insecurity. Efforts to secure cyberspace require greater integration of human rights concerns and analysis of threats to the civil society actors that have tried to address them, as these elements are key factors in the Chinese government's own comprehensive cyber strategy.

State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining

Jeffrey Kwong, Department of Political Science, UC San Diego

The onslaught of cyber attacks waged against American interests domestically and abroad in Japan, Taiwan, and Israel highlights an alarming trend. Non-state, nationalist actors are increasingly coordinating such attacks and often independently from home governments, raising questions as to why these groups attack and why their governments fail to stop these attacks. In particular, I ask questions on the conditions under which non-state activist groups launch politically motivated interstate cyber attacks, especially in the case of China and how the Chinese government is involved. This will help policymakers interpret and develop actionable plans to respond to non-state groups operating within the confines of non-credible authoritarian regimes.

Current definitional issues with "cyber war" and the continual academic study and characterization of cyber attacks as cyber war remain a challenge to the advancement of cyber attacks as a subject of explanation in academic study. I adapt the National Academy of Sciences definition and define cyber attack as the "use of deliberative actions to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks" and/or the "use of cyber offensive actions to support the goals and missions of the part conducting the exploitation, usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks." I argue that political scientists and policymakers should focus attention on those two categories of attacks that are informational and coercive, and where the attacker type can actually be known, especially as politically-motivated cyber attacks have increased dramatically in the past decade.

Table 1. Types of cyber attacks

	Public	**Unknown identity**
Profiteering	Advertisements, spam.	To obtain credit card numbers on Bank of America database; the goal is to utilize credit card numbers for profiteering motives.
Information	Antisec (Anonymous slinter group) To obtain and publicize data from Pentagon through an attack on Stratfor; the goal is to publicize alleged profit motives of U.S. military firms and misinformation of public by U.S. policymakers.	To obtain data from Pentagon through attack; the goal is to reduce informational asymmetries between the Pentagon and unknown parties.
Coercion	Red Honkers Union (China) To disrupt and degrade state websites in United States and Japan; the goal is to increase domestic consciousness on the issues of nationalism and to show domestic resolve to foreign and domestic actors.	To attack Seimens supervisory control and data acquisition (SCADA) systems used to monitor internal industrial systems used by Iranian centrifuges by attacking the programmable logic controller rootkit data; the goal is to increase the costs and disrupt the Iranian nuclear program.

I focus on Chinese politically-motivated cyber attacks: Given the oftentimes anonymous nature of cyber attacks, the different cost structures, the lack of actual payoffs or deals as the endpoint of such attacks, the way capabilities work strategically in the context of bargaining and deterrence, and the divided and disunited role of actors and states as agents, why do Chinese non-state actors make their attacks public and why do governments allow them? Under what conditions do Chinese non-state activist groups launch politically motivated interstate cyber attacks? How are governments involved? How can the United States take action to avoid the escalation of cyber attacks that can fuel territorial conflicts in global hotspots such as the Formosan Strait, Indo-Pak, South China Seas, and the former Soviet Union? How should the United States interpret and develop actionable plans to respond to non-state groups operating within the confines of non-credible authoritarian regimes?

I make the argument that the Chinese state lacks credibility in foreign threats, thus non-state actors launching cyber attacks unsanctioned by Beijing helps make China's threats more credible in the eyes of opponents. I look at how Chinese cyber attacks fit into the picture of an increasing number of politically motivated, public, attributable cyber attacks. I catalog all attacks from 1990 to January 2012—where attackers, targets, and intentions are verifiable—and show that Chinese cyber attacks are tied with state threats against opponents during times of bilateral disputes similar to the way Russian and Iranian citizen hacking groups operate. I also employ regression and statistical analyses to look at three databases including one collected by myself using Korean, Chinese, and English language sites, as well as Indian, Pakistani, Israeli, Japanese, and Turkish news sources with triangulated sourcing from Lexis Nexus World News sources and a subscriber-based Chinese language news database. (This paper also uses data from Zone-H and the University of Nebraska Cyber Attacks database. These databases are partial and my research responds to the need for a more complete and sourced database.)

China allows for the opportunity for non-state controlled launching and planning of cyber attacks to credibly signal coercive threats. The reason why these threats are credible is that since China cannot control these attacks and these attackers are more nationalistic than the state, the attacks impose costs on the Chinese government and threaten to heighten domestic Chinese unrest if the Chinese government makes a threat against Japan or the United States and backs down. In other words, for the authoritarian regime, the risk of cyber attacks is twofold: if the state does not take a more nationalist position, the cyber attackers may turn their anger against their home state. In addition, failure to contain the cyber attacks may increase the risk of actual state-to-state conflict.

China's publicly verified attacks, unlike those in the United States or other Western democracies, are more likely to be publicly identifiable inter-state cyber attacks waged by non-state groups. Timing Chinese cyber attacks with Chinese state threats made by Beijing, there's a clear maneuvering and signaling that the Chinese government is planning and implementing; threats against United States, Taiwan, or Japan are followed by huge cyber attacks raising the audience cost and fortifying the perception among the Chinese public and the opponent state that China is serious about its threats.

In allowing cyber attacks, Beijing can show an adversary they are credible about a threat. Since these cyber attacks are, to a certain degree, independent and controlled by a third party, these attackers can also turn around and utilize their threats against their home state, giving China a credible signaling strategy. For example, Pro-Beijing, Chinese cyber attackers target the Taiwan Ministry of Defense. Beijing reiterates anti-Taiwan rhetoric. However, Beijing does not take action against Taiwan and ultimately, attackers wage a cyber attack against Beijing to express its displeasure. Thus, Beijing takes a risk by allowing attacks and is able to credibly signal to Taiwan its threat's seriousness since it is able to risk its own government and open itself to domestic discontent and disapproval. The risk posed by non-state actors to their home authoritarian regime makes the home state's threats credible (e.g., a red youth Communist loyalist Chinese hacker group attacking sites of the Japanese Ministry of Defense also poses a risk to the Chinese government).

The Project on the Study of Innovation and Technology in China

Innovation, Defense Transformation, and China's Place in the Global Technology Order

Under the leadership of Tai Ming Cheung, The Project on the Study of Innovation and Technology in China (SITC) examines China's drive to become a world-class defense and dual-use technological and industrial power and the security and economic implications of this transformation for U.S. national security. The overarching aims of this project are two-fold: 1) it will provide rigorous analysis and new data on the vital but neglected issue of the nature and trajectory of China's military technological rise; and 2) it will cultivate a new generation of scholars and policy analysts knowledgeable on Chinese security and technology issues. The project is funded by a $9.6 million grant from the U.S. Defense Department's Minerva program.

The primary goals of the five-year project are to: 1) conduct inter-disciplinary investigation into the dynamics of the evolution of the Chinese defense and dual-use science, technology, and industrial (STI) bases; 2) locate this research within a broader functional and comparative framework that contrasts China's experience with other states; 3) address the national security implications of China's military and technological transformation for the United States and international community; and 4) train a new generation of scholars and policy analysts and help develop the field of Chinese security and technology studies. IGCC will partner with the Hoover Institution at Stanford University and Stockholm International Peace Research Institute in these endeavors.

SITC is comprised of six research projects: 1) annual assessments of the reform and modernization of critical sectors in China's defense and dual-use STI base; 2) comparing China's approach to technology development, defense industrialization, and forging of a dual-use base with peer competitors and latecomers; 3) analysis of the political economy of China's defense S&T and technological rise; 4) China's technological development and implications for U.S. and international technology trade policies; 5) the nature of the structures, processes, and leaderships of the Chinese civilian and defense S&T systems; and 6) historical influences on contemporary Chinese grand strategic thinking on S&T.

A relational database project supports quantitative and network analysis of data from these projects. Output includes annual reviews of the Chinese defense STI base, edited volumes, journal articles, working papers, and online briefings. SITC provides internships and fellowships for graduate students and post-doctoral researchers to participate in these projects and encourages them to focus on Chinese security and technology issues in their future careers. SITC also conducts briefings related to Chinese science and technology issues to policy and defense audiences and organizes a two-week Summer Training Workshop on the Relationship between National Security and Technology in China. More information can be found at www.igcc.ucsd.edu/SITC.

The EMC Chair at the Naval War College

Held by Professor Derek Reveron, the EMC Chair serves the Naval War College and the security studies community through cutting-edge teaching and research that explores the intersection between national security and information technology. The Chair engages with leaders from academia, industry, and the Department of Defense to explore how knowledge is created, shared, and managed. With a specific emphasis on intelligence, cyber, and maritime security, the EMC Chair explores information sharing between industry and government and between developed and developing countries.

The Chair designs and implements workshops in the field of cyber studies. Over the last several years, the workshops have been guided by three key questions.

1. What are the cultural, policy, technical, and legal impediments to effective information sharing?
2. What are the limits of current strategies, concepts, organizations, and thinking about cybersecurity?
3. What roles have national cyber capabilities played in contemporary conflict?

In 2010, experts from academia, policy institutions, the IT industry, and the military came together to consider the evolution of threats to cyberspace, discuss methods to defend cyberspace, place cyber operations in the context of international law, and debate visions of cyberwar. In 2011, a diverse group considered how the character of war is changing with respect to cyberspace operations and in particular the connectivity, content, and cognition of the information environment that will impact operational warfare in 2030. Future work with IGCC will continue examining cyber issues in a comparative context to inform future thinking about cyber, conflict, and cooperation.