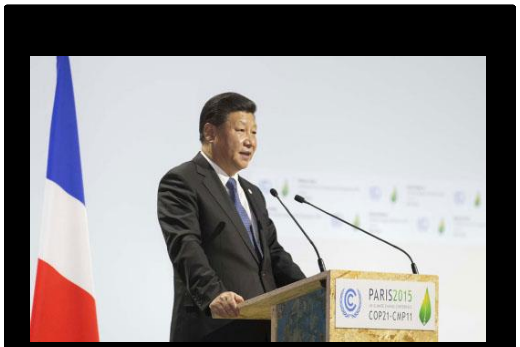
中国简报 China Brief
a journal of analysis and information
The JAMESTOWN FOUNDATION

Volume XV • Issue 24 • December 21, 2015

In This Issue:



Chinese President Xi Jinping speaks at the UN Climate Change Conference in Paris Source (Source: QQ)

China Brief is a bi-weekly journal of information and analysis covering Greater China in Eurasia.

China Brief is a publication of The Jamestown Foundation, a private non-profit organization based in Washington D.C. and is edited by Peter Wood.

The opinions expressed in China Brief are solely those of the authors, and do not necessarily reflect the views of The Jamestown Foundation.

For comments and questions about China Brief, please contact us at wood@jamestown.org

The Jamestown Foundation
1111 16th St. NW, Suite 320
Washington, DC 20036
Tel: 202.483.8888
Fax: 202.483.8337

In a Fortnight

Waking Up? China Moves on Environmental Issues at Paris Summit

By Peter Wood

In 2009, the image of Chinese ministers asleep at their desks at the United Nations Climate Change Conference in Copenhagen was taken as a metaphor for the world's torpid movement on environmental issues. With the results of the recent Paris Conference on Climate Change showing progress and a number of reforms by China's top leadership, it is becoming clear that, in terms of both foreign and domestic policy, China is "waking up" to face its environmental problems.

At the conference in Paris, which ended on December 12, delegates from 196 countries agreed to a framework that, if approved by a majority of top carbon emitters, will become legally binding. China and the U.S., despite their frequent and ongoing disagreements on a number of strategic issues, are viewed as being cooperative partners in this endeavor.

The groundwork was laid during President Xi Jinping's visit to Washington in September. U.S. President Obama and President Xi "reaffirm[ed] their shared conviction that climate change is one of the greatest threats facing humanity and that their two countries have a critical role to play in addressing it" (NDRC, September 26). China committed itself to lowering carbon dioxide emissions per unit of GDP by 60-65 percent from its 2005 level by 2030.

As ever, balancing the needs of economic growth and environmental protection have proven difficult, particularly with a country as reliant on coal for power generation, and whose economy is widely viewed as going through a period of contraction.

Domestically, at the top level, there are positive signs. A White Paper issued by the National Development and Reform Council (NDRC), China's top economic planning agency, acknowledged a range of environmental crises—from droughts and soil degradation to air pollution, paving the way for further action (NDRC, November 2013). Premier Li Keqiang announced at a June meeting of the body that China was on-track to achieve the current five-year plan's carbon-reduction and environmental goals (Gov.cn, June 12). The Leading Small Group for Comprehensively Deeping Reforms (中央深改组), a committee lead by Xi Jinping and members of the Politburo Standing Committee, issued a series of action plans dealing with the environment (Xinhua, July 5). Specifically, these reforms within the Ministry of Environmental Protection (MEP) have shifted responsibility onto local cadres to improve and changed the budget mechanism for local environmental bureaus' (环保局) that had discouraged them from issuing fines. The MEP's new media savvy "scholar-politician" Chen Jining has been a much more effective voice than his predecessors (*China Brief*, December 7). While these moves at the highest level are certainly welcome, facts on the ground paint a different picture.

At the local level, things are less encouraging. China has for many years seen large protests against specific environmental threats, particularly carcinogenic chemical-producing factories. Though these groups have been effective in shutting down polluting factories in Xiamen and Dalian, cities in China's south and north, similar protests elsewhere, including in Kunming and Chengdu, both cities in China's south west, have faced more stern opposition from local governments (SCMP, May 20, 2013). In response to mass protests, the Kunming city government eventually published an environmental report on the proposed factory (*Beijing Morning Post*, June 26, 2013). In each of these cases, government action came only after it became apparent that media suppression and riot control would no longer be effective. Moreover, government action was successful in suppressing these issues from becoming larger, national level movements.

More troublingly, seemingly universal problems, such as urban smog, have failed to mobilize significant protest. Years after the U.S. Embassy briefly labeled Beijing's air as "crazy bad," this month, Beijing issued its first ever smog red alert (ChinaNews Online, December 7; Caixin, December 8). This was quickly followed by a second red alert less than two weeks later (Sina Online, December 18). It appears that most Chinese citizens have chosen to simply don their breathing mask, change the filter of their air purifier and get on with their lives.

The Chinese government, through its restriction of Non-Governmental Organizations (NGOs), lack of support for grassroots environmental efforts and long inattention to environmental issues that could slow economic growth has created a recursive loop of focus on growth, empty promises and apathy. Though China's cooperation in international forums is certainly welcome, without a "comprehensively deep" internalization of environmental protection, from the Politburo to the city block, the needed will to correct China's environmental issues—much less global concerns—will be lacking.

***

China's Draft Cybersecurity Law

By Zunyou Zhou

In early December, China and the United States reached an agreement in their first round of high-level dialogue on fighting cybercrime and other malicious cyber activities (*China Daily*, December 2; *Legal Daily*, December 2). The meeting marked a significant step for both countries in establishing acceptable rules on cybersecurity after Chinese President Xi Jinping and U.S. President Barack Obama signed a bilateral "no-hacking" pact during Xi's state visit to the U.S. in September 2015.

The cybersecurity agreement brought international attention again to China's Draft Cybersecurity Law unveiled by the Standing Committee of the National People's Congress (NPC) on July 6, 2015 (NPC website). The 68-article draft law was released shortly after the passage of China's revised National Security Law and the publication of two other draft laws on counterterrorism and NGO management. All four laws are considered an ambitious effort by the Chinese Communist Party (CCP) under Xi Jinping's leadership to maintain its firm grip on power in a changed domestic and international environment. Against this backdrop, it is important to take a careful look at the legislative background and the text of the draft law to understand China's views of the risks posed by cyberspace and the policies it will implement to cope with these risks.

Legislative Background

An explanatory of the draft law suggests as justifications for this proposal "new situations," "[the] CCP Central Committee's requirements" and "people's expectations" (NPC website, July 6).

– "New situations" are a reference to: (1) cyber-attacks threatening the security of critical information infrastructure in the sectors of telecommunication, energy, transportation, finance, national defense and public administration; (2) unlawful actions, such as illegal acquisition, release, purchase, or sale of personal data, insulting or slandering other people, and violating intellectual property, which seriously violate the legitimate rights of natural persons or legal entities; (3) dissemination of illegal information propagating terrorism or extremism and instigating the subversion of state power or overthrow of the socialist system, or spreading of pornographic information.

– "CCP Central Committee's requirements" include: (1) "new thoughts, new opinions and new judgments" by President Xi Jinping; (2) the suggestions of the Fourth Plenary Session of the 18th CCP Central Committee for improving cybersecurity.

– "People's expectations" are obligations put on the authorities to: (1) strengthen cyberspace governance according to law; (2) regulate the transmission of Internet information; (3) suppress violations and crimes in cyberspace; (4) create a transparent and safe cyberspace.

The explanatory report also points out the draft law's "guiding thoughts" that include the "overall national security outlook" (总体国家安全观) proposed by Xi Jinping and the Chinese Internet policy of "active use, scientific development, law-based administration and ensured security" (Xinhua, April 20; *China Brief*, July 17; People's Daily Online, June 8, 2010).

Cybersecurity Administration of China

A key point of the draft law is the suggestion of a leadership role for the Cybersecurity Administration of China (CAC) for maintaining security in cyberspace. Pursuant to Article 6 of the legislation, the CAC is responsible for planning, coordinating, supervising, and administering cybersecurity-related affairs. Accordingly, other governmental organs such as the Ministry of Industry and Information (MIIT) and the Ministry of Public Security (MPS) may discharge their own duties in accordance with this law and other regulations. The CAC, therefore, will be elevated to the role of China's paramount Internet security regulator.

Aside from the general authorization granted under Article 6, the CAC's specific tasks and powers also include: (1) handling complaints about harmful acts against cybersecurity (Article 10); (2) designating critical Internet equipment and specialized cybersecurity products (Article 19); (3) organizing security inspections of Internet products and services purchased by critical information infrastructure operators (Article 30); (4) setting security assessment rules on the admissibility of storing personal information and other important data outside Chinese territory (Article 31); (5) developing coordination mechanisms for security testing, emergency drills, information sharing, and technical assistance for protecting critical information infrastructure (Article 33); (6) requiring Internet service providers (ISPs) to stop or block the transmission of information prohibited by law (Article 43); (7) coordinating the collection, analysis and reporting efforts with regard to Internet security information (Article 44).

The CAC, also known as the Office of the Central Leading Group for Cybersecurity and Informatization, is headed by Lu Wei, who also serves as the deputy head of CCP Propaganda Department, an internal CCP organ in charge of ideology-related work. This Central Leading Group, headed by Xi Jinping, is a decision-making body of the CCP Central Committee for formulating and implementing policies on cyberspace affairs. The group's two deputy heads are Li Keqiang, Premier of the State Council, and Liu Yunshan, chief of the CCP Propaganda Department. Lu's position within the CCP as a top propaganda official implies that the CAC's main task is to censor the cyberspace.

At the first meeting of the Central Leading Group in February 2014, Xi Jinping called for a dual focus on "cybersecurity" (网络安全) and "informatization" (信息化, "advancing information technology"), arguing that "without cybersecurity, there is no national security; without informatization, there is no modernization" (Xinhua, February 27, 2014).

According to Article 1 of the draft law, the legislation's objectives are fourfold: cyberspace sovereignty, social stability, privacy protection, and economic development. As such, the first objective is to provide a legal basis for preserving China's "cyberspace sovereignty" (网络空间主权), also known as "cyber sovereignty" (网络主权).

Cyberspace Sovereignty

The proclamation of cyberspace sovereignty may date back to a 2010 Chinese government white paper on Internet policy, whose core tenet was that "the Internet is an important infrastructure facility for the nation" and "within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty" (*China Daily*, June 9, 2010). China's intention to uphold cyber sovereignty has also been written into its 2015 white paper on military strategy, which characterizes cyberspace as a new domain for national security and announces China's preparation for strengthening its cyber military forces (Xinhua, May 26; *China Brief*, June 23). From the perspective of the Chinese government, while the Internet is global in nature, how it is governed should be subject to the jurisdiction of each country. President Xi Jinping reaffirmed the principle of cyberspace sovereignty in his most recent keynote speech at the Second World Internet Conference held in China (Xinhua, December 16).

According to Ye Zheng, an information warfare expert with China's Academy of Military Science, cyber sovereignty is a new concept first proposed by China and subsequently opposed by some Western countries. But this concept is gradually finding acceptance in the international community, including some Americans. In this regard, the current contention is not on whether sovereignty in cyberspace exists, but on how it is interpreted and safeguarded (People's Daily Online, July 20).

The China-U.S. debate over cyberspace sovereignty is linked to the global controversy on Internet governance. Growing discomfort with the dominance of the United States in global cyberspace and its use of cyber capabilities has prompted China to pursue actions directed at changing the status quo of global Internet governance. China's recent submission, together with like-minded allies in the Shanghai Cooperation Organization (SCO), of an updated version of the International Code of Conduct for Information Security to the United Nations in January 2015, is one such example (*China Brief*, September 4). **[1]**

Cyberspace Censorship

Another major objective of the draft law is to maintain "social stability." This concern is so serious that it is, in the lexicon of the CCP, synonymous with "national security" as seen through the lens of Xi's comprehensive national security concept (*China Brief*, November 16). In his explanatory report on the resolution by the Third Plenary Session of the 18th CCP Central Committee on major issues concerning comprehensively deepening reforms, Xi stressed the importance of reforming Internet management. In Xi's opinion, the driving force of the reform is the challenge to "national security and social stability" posed by the rapidly growing number of social network users and instant messaging tools characterized by fast communication, high influence, broad coverage, and strong mobilizing capability (Xinhua, November 15, 2013).

In order to promote social stability, the draft law dedicates the entire fourth chapter, entitled "Internet information security" and comprised of 10 articles, to this issue. While Articles 34–39 are designed to protect personal information, Articles 40–43 are measures for censoring illegal information.

In terms of privacy protection, ISPs are required to meet their legal obligation to protect personal information (Article 34). Thus, the ISPs must follow principles such as legality, legitimacy and necessity (Article 35). They are also required to adopt measures necessary to keep the personal information collected strictly confidential (Article 36). An individual has the right to request the deletion of his or her personal information collected or used by the ISPs (Article 37). Nobody is allowed to acquire or disclose the personal information of others in an illegal manner (Article 38). Government authorities must not disclose any personal information obtained while performing their duties (Article 39).

As for censorship measures, ISPs are obligated to stop the spread of information prohibited by law (Articles 40 and 41) and to set rules for handling complaints on Internet information (Article 42). The CAC and other public offices are empowered to order ISPs to block the transmission of such illegal information (Article 43).

It is surprising to note that, while the first half (Articles 34–39) of the fourth chapter is devoted to the protection of cyberspace privacy, the second half (Articles 40–43) lays down the obligations of ISPs and the powers of government agencies in censoring all illegally collected or used information, whether personal or non-personal. The fact that all these provisions are gathered in one chapter begs the question of whether the law is really meant to protect cyberspace privacy or, rather, is intended to carry out Internet censorship under the pretext of privacy protection.

Another reason for skepticism is that this law has other provisions, outside the fourth chapter, that may be used for cyberspace censorship. For example, Article 20 requires Internet users to register in their real names in order to receive Internet services. Article 50 of the draft law goes even further, allowing the government to temporarily shut down Internet access in areas where public security is deemed to be threatened.

These censorship measures may be necessary and even useful for maintaining order in cyberspace, but they will also disproportionately infringe on the freedom of speech of Internet users.

Cybersecurity with Chinese Characteristics

The Chinese concept of cybersecurity was clearly articulated in a 2013 speech by Lu Wei. This involves four concepts: security of cyberspace sovereignty, security of Internet information, security of privacy in cyberspace, and security of information technology (Xinhua, December 10, 2013). It is necessary to note that basic rights such as privacy are often interpreted as defensive rights of citizens against state intervention. Since, in many cases, individual privacy and national security are by nature in conflict, the so-called "security of privacy," an elusive term coined by Lu, is doomed to be a mission impossible.

The Chinese cybersecurity bill needs to be understood in the context of China's rise in economic strength and global influence and its aspiration to set norms in global affairs. By attempting to create borders in cyberspace and solidify the status of the CAC as the leading organ for governing the cyberspace, the draft law demonstrates the CCP's resolve to protect national interests in the face of international pressure.

A review of the draft law reveals that while the list of powers granted to the government is long, only one obligation is imposed under Article 39 (see above); the obligations imposed on Internet service providers and Internet users are numerous, but no rights are granted to the providers and only one to the users under Article 37 (see above). According to Xie Junzhe, a cybersecurity law expert with Renmin University of China (RUC), the draft law leaves the impression that it deals solely with questions of how the government may rule the cyberspace and how companies and individuals need to cooperate with the government (China Civil and Commercial Law Net, July 19). This leaves the question of how will rights be protected. As Xie's colleague at the RUC, Professor Liu Pinxin, argues, the law needs more provisions on the protection of fundamental rights in order to balance the interests of security and liberty in the cyberspace (People's Daily Online, September 1).

Conclusion

The sweeping and vague draft law on cybersecurity gives the Chinese government almost unbridled powers to maintain the nation's security in cyberspace. If the draft law in the current form is passed and the discretionary powers enjoyed by the government are not balanced by strict conditions and strong oversight, it remains questionable whether the security, achieved at the expense of fundamental rights, is genuinely worthwhile.

Dr. Zunyou Zhou is a senior researcher and head of the China section at Germany's Max Planck Institute for Foreign and International Criminal Law and the author of "Balancing Security and Liberty: Counter-Terrorism Legislation in Germany and China" (2014).

Notes

1. *Wang Xiaofeng, The Issue of Cybersecurity in the China-U.S. Relationship, in: American Studies, No. 3, 2013 [汪晓风, 中美关系中的* 网络安全问题, 《美国研究》2013 年第 3 期], pp. 20–24).

***

The Latest Indication of the PLA's Cyber Warfare Strategy?

Comparing the Strategic Guidance for Military Struggle in Cyberspace from the 2013 and 2015 editions of *The Science of Military Strategy*

By Elsa B. Kania

The 2015 text of *The Science of Military Strategy* (战略学), published by the PLA's National Defense University (NDU) in April, offers an interesting contrast with the 2013 Academy of Military Science (AMS) edition. These authoritative texts, which are used as teaching and reference materials for senior PLA officers, articulate the PLA's thinking on and approach to military strategy in multiple domains and contexts. **[1]** Since the AMS has a more direct role in the formulation of military strategy, the 2013 text of *The Science of Military Strategy* might be more authoritative than the 2015 edition. **[2]** However, this NDU text also presents an influential perspective that merits closer examination. **[3]** Notably, the 2015 text includes not only sections on 'military struggle in cyberspace' (网络空间军事斗争) and network-electromagnetic space operations (网络电磁空间作战) but also a full chapter on measures to establish and develop the PLA's cyberspace forces. **[4]**

There are sections within this 2015 text that seem to reflect a relatively distinctive approach to certain issue areas, including military struggle in cyberspace. The various differences and divergences between these two texts might indicate variance in perspective at the institutional level and/or a discernible change in the PLA's recent strategic thinking on conflict in this new domain. **[5]** Although this limited, preliminary comparison of the 2013 and 2015 texts hardly allows for a definitive assessment of the potential shifts in China's strategic thinking on cyber warfare during this timeframe, this recent edition of *The Science of Military Strategy* does introduce certain concepts that are new relative to the 2013 AMS text, including the prioritization of defending China's cyber sovereignty (网络主权) and "cyber borders" (网络边疆), while also articulating the intention to establish a "cyberspace forces leadership structure" (网络空间力量领导体制), analogous to U.S. Cyber Command. **[6]**

New Perspectives on Cyber Reconnaissance and Cyber Deterrence?

At a basic level, the AMS and NDU texts differ in their respective categorizations and definitions of the forms of cyber warfare, especially with regard to cyber reconnaissance and cyber deterrence. **[7]** In the 2013 text, cyber reconnaissance is discussed as inherently related to and potentially the precursor for cyber attack; in the 2015 text, on the other hand, the espionage-related aspects of cyber reconnaissance are emphasized. By the AMS text's characterization, cyber reconnaissance is typically "the preparation for probable future cyber attack operations." However, the 2015 text does not mention the technical or operational linkages between cyber reconnaissance and cyber attack. Rather, according to that text, "cyber espionage struggle has become the most apparent form of peacetime military struggle in cyberspace." Here, the U.S. National Security Agency's program Prism is discussed as an indication of the extensiveness and sophistication of U.S. cyber espionage activities. This allusion to U.S. cyber espionage and the addition of "counter-reconnaissance" could perhaps reflect the impact of Edward Snowden's revelations upon the PLA's perceptions of China's vulnerability to U.S. cyber capabilities.

While the 2013 and 2015 texts each recognize the strategic significance of cyber deterrence, this concept is seemingly more highly prioritized and discussed with additional nuance in the 2015 text. As of 2013, there was uncertainty associated with the AMS characterization of cyber deterrence; at that time, the authors mentioned that the existence of "very large differences" of opinion on cyber deterrence, such that the "theories and practice of cyber deterrence" were 'still pending improvement' and required further development. On the other hand, in the 2015 text, cyber deterrence is discussed with less uncertainty and divided into strategic and tactical levels. According to the NDU text, "strategic-level cyber deterrence" (战略级网络威慑) involves the demonstration of cyber attack capabilities, which would have massive destructive power if used against an enemy's political, military, and economic targets, including C4ISR systems, while "tactical-level cyber deterrence" (战术级网络威慑) primarily entails the use small-scale cyber attacks in order "to ensure the maintenance of national security in peacetime." Notably, this discussion of tactical-level cyber deterrence seems relatively unique, compared to previous such publications, which may reflect the PLA's concern with deterring not only large-scale cyber attacks but also lower-level cyber threat activities. However, the actual operationalization and potential efficacy of such an approach to cyber deterrence is another question entirely.

Comparing the 2013 and 2015 Texts' Strategic Guidance for "Cyber Military Struggle"

The strategic guidance (战略指导) for this new form of military struggle evolved between the 2013 and 2015 texts, and it is notable that each articulates a relative emphasis on defense. Nonetheless, each text also emphasizes the criticality of the "cyber battlefield" to winning future informationized wars in this and other sections of the text. The NDU text asserts, "victory in war first starts from victory in cyberspace; whoever seizes the initiative in cyberspace will win the initiative in war." Concurrently, there is also, however, a defensive orientation relative to the PLA's previous strategic guidance on cyber warfare, which, as of the 2001 text of *The Science of Military Strategy*, under the aegis of strategic information operations, included the exhortation to "gain the initiative through striking first and seize the decisive opportunity" (先发制人, 掌握先机), while implementing "active offense" (积极进攻). However, as of the 2013 or 2015 editions, the PLA's concept of 'military struggle in cyberspace' appears more directly linked to its overall strategy of active defense, despite still emphasizing an offensive approach to cyber warfare in a wartime scenario.

In the 2013 text, the first strategic guidance is to "establish the protection of the safety of the nation's important information and information networks as the fundamental objective." **[8]** This clear emphasis on the defensive is followed by a second strategic guidance to "manage well' the relationships of peacetime and wartime, attack and defense, and deterrence and warfare in cyber confrontation. Under the aegis of this guidance, the authors note that relative to its "primary strategic adversary," implicitly the U.S., China is inherently at a disadvantage in cyber confrontation, such that it should "give priority to defense; give simultaneous consideration to attack and defense" (以防为主, 兼顾进攻). Although this emphasis on defense doesn't detract from the focus on offense and potentially even preemption in the scenario of an informationized war, the strategic guidance as listed does seem to indicate the PLA's intensified concerns about its relative vulnerability and the necessity of enhancing its defensive capabilities.

After the preceding two points, the third element of the guidance listed in the 2013 text, which discusses the PLA's intentions to establish three forms of "specialized cyber operations forces" (专业网络作战力量), should not necessarily be assessed as an indication of predominantly offensive intentions, since such forces could have both offensive and defensive applications. These three types of cyber forces are "specialized military cyber warfare forces" (军队专业网络战力量); "PLA-authorized forces" (授权力量); and civilian forces (民间力量), as has been previously discussed (*China Brief*, April 16). **[9]** This commitment to developing and advancing China's cyber forces and capabilities is also reaffirmed and further detailed in the NDU's 2015 text.

Looking now to the strategic guidance for cyberspace military struggle within the 2015 NDU text, the first listed elevates the defensive orientation evident in the 2013 text to an even higher level, with the exhortation to "defend cyber borders; guard cyber sovereignty and national security" (守卫网络边疆, 捍卫网络主权和国家安全). Although the concept of "cyber sovereignty" (网络主权) has been increasingly prioritized by and prevalent in the statements of China's civilian leadership, including during the recent World Internet Conference in Wuzhen, this is apparently the first time that this concept has been used in a PLA publication with this level of authoritativeness (*China Brief*, September 4). So too, the notion of cyber borders (网络边疆), while previously discussed in the broader PLA literature, especially in the writings of Major General Ye Zheng, a member of the PLA's Strategic Advisory Committee and an influential information and cyber warfare theorist, is also new relative to the 2013 text. **[10]** Here, the authors argue, "cyber[space] lacks borders, but has sovereignty." Their starting point for asserting the importance of protecting cyber sovereignty is the Arab Spring, with the argument that cyber sovereignty is essential to prevent an enemy from 'engineering societal chaos' and to maintain political stability. In this regard, the PLA's strategic guidance is directly linked to the CPC's priority of preserving stability to ensure its own predominance and survival. **[11]**

Next, the 2015 text sets forth the guidance of "active defense; contain [and] win future wars" (积极防御,遏制并打赢未来战争). Consistent with multiple previous PLA publications, "seizing cyber superiority" (夺取网络制权) and information superiority are seen as the foundation for seizing battlefield superiority in its entirety. Here, in the context of a potential conflict, there is an emphasis on the cyber-attack as a means to achieve victory. Nothing that multiple nation-states, including the U.S., have developed offensive cyber strategies, the authors argue that there is an imperative for active defense, as well as an emphasis on "integrated deterrence and warfare" (慑战一体). This framing of China's approach to military struggle in cyberspace within the context of the PLA's overall strategy of active defense, which is strategically defensive but can be operationally and tactically offensive, is clearer than in previous such publications. This emphasis on active defense indicates that the PLA might justify the use of offensive cyber campaigns and tactics as defensive, even an integral element of national defense, at the strategic level.

Questions for Future Analysis:

Such an initial comparison of the 2013 and 2015 editions of *The Science of Military Strategy*, while only a preliminary step in support of more comprehensive analysis of these authoritative new texts, seems to offer indications of potential changes in the PLA's strategic thinking on cyber warfare during this timeframe. Certainly, the implications of these competing or perhaps complementary texts, as well as their relative authoritativeness, remains a question for further consideration. So too, the realization at the organizational and operational levels of the strategic concepts and theories articulated in these texts remains to be seen. However, at the strategic level, the inclusion of the concepts of cyber sovereignty and cyber borders, as well as the clear linkage of the PLA's approach to military struggle in cyberspace with its overall strategy of active defense, offers insights on the PLA's evolving strategic thinking on cyber warfare.

Notably, in a later chapter of the 2015 text, there is discussion of specific measures to advance the development of China's cyber forces, including the establishment of a "authoritative, unified leadership and command organization" (权威的统一领导指挥机构). This section seems to support previous articulations of and recent reports regarding the PLA's intentions. Even the 2015 defense white paper on "China's Military Strategy," a document intended for and presented to an international audience, had emphasized that China must "expedite the development of a cyber force" (State Council Information Office, May 26). Against the backdrop of announcements on the PLA reform agenda, there have also been media reports that China will seek to consolidate its cyber warfare units, which are currently dispersed across multiple units and ministries, into a command that would report directly to the Central Military Commission (Bloomberg, October 22). Perhaps, as PLA reforms progress, there could be an official announcement of the establishment of such a command, which would offer the necessary clarity regarding such a substantive organizational change in the PLA's approach to cyber warfare.

Elsa Kania is currently a senior at Harvard College and works part-time as a research assistant at the Belfer Center for Science and International Affairs. She was a 2014-2015 Boren Scholar in Beijing and previously worked as an intern in the cyber security industry.

Notes

1. See M. Taylor Fravel's "The Evolution of China's Military Strategy: Comparing the 1987 and 1999 Versions of ZHANLÜEXUE" (2005) for a detailed comparison of earlier editions of these texts and further discussion of their authoritativeness. *China's Evolving Military Strategy* (2016) will offer a comprehensive analysis of the AMS' 2013 edition of *The Science of Military Strategy*.

2. Thank you to Larry Wortzel and Joe McReynolds for sharing helpful insights regarding this 2015 text's relative authoritativeness.

3. For instance, whereas the 2013 text was released in the name of a committee of authors, under the aegis of a particular research department, the names of the individual authors of various chapters are listed for the 2015 text.

4. Although the Chinese word that is typically translated as "cyber" (网络) literally means "network" and does not correspond precisely with the U.S. concept, I will use the prefix "cyber" in my translations of these terms for the purposes of this article.

5. At a very basic level, there is a divergence in the terminology used in the 2013 AMS and 2015 NDU texts of *The Science of Military Strategy*. The AMS frequently refers to the cyber *domain* (网络领域), but the NDU consistently uses the term cyber *space* (网络空间) instead. Although this two-character difference might seem trivial, this terminological divergence might reflect that the AMS perceives the cyber domain as a distinct domain of warfare, whereas the NDU might instead perceive "military struggle in cyberspace" primarily as an element of and force multiplier for conventional warfare. However, this slight difference could also reflect that there have simply been different terms used for comparable concepts, as has also occurred in a U.S. context.

6. Although the concept of cyber sovereignty, as well as that of cyber borders, has previously been discussed in the PLA literature, as well as extensively by China's civilian leadership, this is, to my knowledge, the first time that these concepts have been introduced into a military text with this level of authoritativeness.

7. While the 2013 text discusses cyber reconnaissance (网络侦察), cyber attack and defense operations (网络攻防作战), and cyber deterrence (网络威慑), the 2015 text discusses first cyber deterrence, then cyber reconnaissance and counter-reconnaissance (网络侦察与反侦察), and finally lists cyber attack and cyber defense separately.

8. Specifically, by the authors' characterization: "China's objective for military struggle in the cyber domain is *self-interested but not harmful, involving evidently defensive, not damaging features*. The aim of China's cyber domain military struggle…is to restrict the scope of an adversary's cyber attack [and] limit the influence of an enemy's cyber destruction to within a scope that our side can endure." [emphasis added]

9. Since this guidance seems to direct that such forces be *established*, it might perhaps be interpreted as articulating the PLA's intention and objective, which is likely in some stage of actualization, rather than a finalized, *status quo* configuration of forces. For instance, the text characterizes forces within civilian government ministries as under the PLA's authorization, but the PLA's actual command and control of those forces might still be subject to debate and pending future consolidation and reorganization

10. See, for instance, "对网络主权的思考" by Ye Zheng (叶征), published in the August 2015 edition of China Information Security.

11. With regard to the CPC's priorities in this regard and for a more expansive discussion of China's cyber strategy, see: Amy Chang, "Warring State: China's Cybersecurity Strategy," December 3, 2014; Perhaps, the elevation of the concept of "cyber sovereignty" in this context might even be interpreted as an indication that Beijing is starting to conceptualize the defense of its cyber borders as associated with its national

core interest (核心利益) of sovereignty and territorial integrity.

***

New Tensions, Old Problems on the Sino-Indian Border

By Ivan Lidarev

As China deepens its economic and strategic relations with Pakistan, and makes diplomatic in-roads with Nepal and Myanmar, it is worth examining an issue that continues to mar Sino-Indian relations. The China-India border dispute has long stirred tensions between Beijing and New Delhi, in spite of regular attempts to put the border issue on the backburner. However, provocative incidents continue to occur between Chinese and Indian forces along the vaguely demarcated and often disputed Line of Actual Control (LAC).

The latest major such incident between the two sides took place on September 11 near Burtse, situated on the far western end of the roughly 3488 kilometer (km) long LAC, between the Ladakh region of the Indian state of Jammu and Kashmir and Xinjiang province. After receiving information that the Chinese were constructing a hut with a camera, Indian soldiers and border police demolished the structure, in spite of Chinese attempts to push them back. This resulted in a stand-off between the two sides.

As it often happens with incidents on the border, the stand-off provoked a small storm of attention from the Indian media, but was downplayed by the Indian government and completely ignored by the Chinese one (Ministry of Foreign Affairs, September 14). Unusually, however, a week after the stand-off had ended a Chinese military spokesperson criticized India for not following border agreements (Ministry of National Defense, September 24). Eventually, the two sides called two “flag meetings” between senior officers, a mechanism for addressing border incidents at five meeting points along the LAC, and resolved the incident (Daily Excelsior, September 15). Both sides agreed to pull out their soldiers and, in what was seen as success for India, abstain from building structures on the disputed LAC.

What made the incident significant was its place and timing. The Chinese provocation took place just before the Indian Home Minster, Rajnath Singh, seen as a hawk on the territorial dispute, was scheduled to make a highly-symbolic visit to the disputed border close to the location of the incident. The minister subsequently postponed his visit to later in September (Times of India, September 13). The location of the incident was also interesting because the area around Burtse is of great strategic significance. It is close to both the G219 and G314 highways. The latter of these is better known as the Chinese part of the Karakorum highway, one of the major arteries through which Chinese aid and personnel come to Pakistan. **[1]** Burtse is also close to India’s small but strategic Daulat Beg Oldi airbase, which New Delhi activated in 2008 to Beijing’s displeasure, and not far from the site of a severe border standoff in 2013 (India Today, August 20, 2013).

The Border Dispute

The Burtse stand-off is just one of a long string of incidents which mark the decades-long border dispute. The dispute concerns three areas around the border 1) the western sector, known as Aksai Chin, which is mostly occupied by China; 2) a middle sector where there are relatively small disagreements on where the border should run; 3) and the fiercely disputed Eastern sector, which is occupied by India and largely covers the Indian state of Arunachal Pradesh. In the middle sector the dispute also concerns Sikkim, a strategically located Indian state which Beijing has not recognized, unequivocally, as part of India. **[2]**

With roots stretching back to the 19th and early 20th century, this dispute was inherited in the 1950s by the recently established People’s Republic of China and a newly independent India. China’s subsequent consolidation of control in Tibet resulted in the gradual souring of the Sino-Indian relationship. The nadir came in 1962, when, in response to India's seizure of territory, China attacked India and inflicted a heavy, albeit limited, defeat on Indian forces. The brief war has adversely shaped mutual perceptions to this day, and has turned the dispute into a highly sensitive issue, especially for India.

Several pushes have been made to resolve the dispute since the 1980s, most notably in 2003, when the two sides initiated the Special Representatives Talks headed by India's National Security Advisor and China's State Counsellor responsible for foreign policy, and in 2005, when the two parties agreed on a set of guidelines for resolving the dispute. **[3]** Nevertheless, in spite of eighteen rounds of such talks, regular declarations that both sides seek to settle the dispute, and years of work of a Joint Working Group on the boundary dispute, there has been little progress toward a final settlement. Instead, focus has increasingly shifted to managing the frequent border tensions.

A quick review of the borders would suggest that China and India can easily accept the status quo and swap their claims over Aksai Chin and Arunachal Pradesh. Nevertheless, a key obstacle is the nexus between the dispute and the issue of Tibet. Beijing's territorial claims are based on the logic that Tibet has been part of China, and India's case is founded on agreements signed by a Tibetan government and British India without Beijing's consent, particularly the 1914 Simla Accord determining the McMahon Line which delineates the eastern sector of the border. Hence, accepting a territorial swap or the legitimacy of some parts of the LAC, which is partly based on the McMahon Line, will bring up the issue of the historical status of Tibet. The Tibet question also involves another great impediment to resolving the dispute, Tawang, a border town with a Tibetan Buddhist monastery that had historically been a part of Tibet and where the next Dalai Lama could reincarnate in the future. Predictably, these characteristics have made the Indian-controlled Tawang a requirement for Beijing in any border settlement. Some analysts have additionally noted domestic constraints on both sides, strategic concerns and the potential that the two sides deliberately want to keep the dispute unresolved.

Incursions

While the border dispute cannot be resolved, it cannot be put on the backburner, either. The reason are the incidents, usually incursions, which regularly take place on the border. On average, about 400 such incidents occur every year, starting in 2012, although the number might be somewhat on the decline this year. **[3]** Most incidents are the result of Chinese patrolling beyond the LAC or the building of small structures, such as huts, bunkers or surveillance installations, by either side.

The last years have witnessed several major incidents. The largest was a three-week stand-off at Daulat Beg Oldi in April and May 2013 which witnessed Chinese soldiers set up tents 19 km inside India-controlled territory in the run-up to the visit of India's foreign minister to Beijing and the visit to India of Chinese Premier Li Keqiang (Economic Times, May 7, 2013). When incident was resolved, in a deal about which little is known to this day, India destroyed a number of bunkers that its troops had recently built on the LAC (The Indian Express, May 13, 2013). Another standoff took place in September 2014, just before President Xi Jinping's trip to India when, in response to Indian construction of a hut with a surveillance camera on the border and the digging of a canal, Chinese soldiers moved to disputed territory in Ladakh to build a road (Times of India, September 24, 2014). An incident also took place in November when a PLA light-armored vehicle went patrolling beyond the LAC during the Indian home minister's visit to Beijing and just days before a meeting between President Xi and Prime Minister Modi at the G-20 summit in Turkey (The Hindu, November 19).

Three features characterize border incidents. First, the incidents have grown since 2007, a development which has led some analysts to connect China's behavior with the U.S.-India nuclear deal and the Tibet uprising of 2008. Second, there has been a particular increase in incidents in the western sector, usually around Ladakh. Third, larger incidents tend to precede high-ranking bilateral meetings, which might suggest that Beijing is using incursions to gain advantage in negotiations or signal its position. The last point leads to the fundamental question why China seeks to provoke border tensions. Explanations have varied from a strategy to keep India on the defensive or punish it for its closer ties with Washington, to a form of coercion on the dispute, to the provocative behavior of local Chinese commanders. Beijing, itself, often explains the incidents with the undetermined LAC, an explanation supported by some independent analysts, although Chinese observers have also sometimes suggested that Indian media deliberately exaggerates the incidents (Global Times, September 15).

Repeated attempts have been made to manage border tensions, starting with the 1993 agreement in which both sides state "No activities of either side shall overstep the line of actual control" (UN, September 7, 1993). More recently, in 2013, China and India signed the Border Defense Cooperation Agreement, which adopts measures to reduce tensions, such as flag meetings between officers at designated points, the proposed establishment of a hotline between the two regional military headquarters, on the two sides of the LAC, and prohibitions against tailing the other side's patrols (Ministry of External Affairs, October 23, 2013). In 2012, the two countries' ministries of foreign affairs also established a Working Mechanism for Consultation and Coordination on India-China Border Affairs between senior diplomats (Ministry of External Affairs, January 17, 2012). The issue has also been discussed regularly at high-level meetings, most recently during a visit to Beijing by India's home minister and during the visit of a Chinese military delegation led by Fan Changlong, Vice Chairman of the Central Military Commission, to New Delhi (NDTV, November 20; Ministry of National Defense, November 16). Nevertheless, neither agreements nor bilateral diplomacy have succeeded in decisively reducing tensions.

Border Infrastructure Building

Beside border incidents, which receive most media attention, border tensions are fueled by an infrastructure building race. This infrastructure building, which has accelerated dramatically in the last ten years, serves three goals: 1) integration of the disputed territories under control; 2) establishment of sovereignty through facts on the ground; and 3) setting up the necessary infrastructure for moving troops and equipment to the LAC fast, in case of armed conflict.

On the Chinese side, as part of a huge project for developing Tibet, Beijing has built a network of roads that reaches every county in Tibet and connects with four main highways, the Central Highway, the Eastern Highway, the Yunnan-Tibet Highway and the Western Highway which eventually extends into the China-Pakistan Karakoram Highway and passes through India-claimed Aksai Chin. **[5]** Many of the roads of this network run very close to the LAC and even beyond it (or what India claims as LAC), such as the Chip Chat Heights road in the western sector, which is four kilometers inside Indian occupied territory. **[6]** China plans to extend this highway network from about 70,000 km in 2013 to 110,000 km by 2020 (China Tibet Online, February 19, 2013; Xinhua, July 29, 2013). China has also been extending its rail lines up to or close to the border. One line between Lhasa and Xigaze, next to Sikkim, was completed in 2014 (with plans for extension to the border), and work has been going on lines to Yatung, next to Sikkim and the strategic Nathula Pass, and Nyingchi, on the border with Chinese-claimed Arunachal Pradesh (Xinhua, August 15, 2014). **[7]** Beijing has also built five airbases in the area around the borders, numerous landing strips and oil depots. **[8]**

Indian infrastructure building has also progressed, although at a much slower pace and from a lower starting point, due to decades-old fears that China could use infrastructure to its advantage in case of attack. Since 2006, New Delhi has initiated a major program of building 73 all-weather roads and 14 rail lines on the border. However, as of 2014, only 18 roads and none of the rail lines have been completed (Times of India, February 20, 2014). In terms of

Advanced Landing Grounds, India has fared better with five airstrips operational by the end of 2014 and two more projected (New Indian Express, September 9). The slow progress on the Indian side has been attributed to bureaucratic inertia, the complex politics between the central government and the states in which the infrastructure is to be built and the fact that several different agencies work on these projects. On his visit to the border at Ladakh after the Burtse incident, Home Minister Rajnath Singh promised the prompt construction of three strategic new roads in the increasingly contested Ladakh region (The Tribune, September 23). This comes on top of a Home Ministry plan of building 27 new roads, a proposed $6 billion new highway in Arunachal Pradesh and suggestions that India might inaugurate a program of population settling in the disputed territories (Mint, October 26).

As the overview above demonstrates, China is far ahead of India in terms of building strategic infrastructure. In case of military conflict, it is estimated that China can presently transport up to 32 divisions in six weeks, along with heavy equipment, all year round and sustain them, from a previous limit of 22 divisions mobilized in six months and not during all times of the year. **[9]** Such a mobilization would leave Indian forces outnumbered 3:1 (Times of India, August 22, 2014). However, India has been increasingly worried by this disparity and has sought to accelerate its infrastructure building, especially as it discusses plans to raise up to two new divisions on the border, three artillery brigades and three armored brigades (The Hindu, April 30).

Conclusion

The Burtse incursion in September is one of a long string of incidents on the Sino-Indian border which often coincide with major bilateral meetings. These incidents, and the race between China and India in building border infrastructure, regularly generate tensions on the LAC and trouble Sino-Indian relations. Efforts to manage such tensions have been consistently unsuccessful. Hence, a more stable relationship between Beijing and New Delhi will require either a real breakthrough in managing border tensions or a resolution of the dispute which underlines them. Neither seems likely in foreseeable future.

Ivan Lidarev is a Ph.D. student at King's College London (KCL) and an advisor to Bulgaria's National Assembly. Ivan's research, published in The Diplomat and Eurasia Review among other publications, focuses on Chinese foreign policy, Sino-Indian relations and Asian security.

Notes

1. Indian media describes Indian military forces in the area around Burtse as capable of monitoring activity on the Karakorum highway. Given the distances and rough terrain, it is uncertain how accurate this information is, but could include signals intelligence.

2. For a brief but comprehensive presentation of the dispute see David Scott "Sino-Indian territorial issues: The Razor's Edge" in Harsh Pant (ed.) *The Rise of China: Implications for India*, (New Delhi: Cambridge University Press, 2012).

3. Alka Acharya "Course Correction: An Analysis of the Origins and Implications of the Sino–Indian Agreements of 2003 and 2005," *China Report,* May 2011, vol. 47: no. 2, pp. 159–171.

4. Catherine Richards, *China-India: An Analysis of the Himalayan territorial dispute*, Centre for Defence and Strategic Studies, Australian Defence College, 2015, p.14

5. Mukul Raheja, "Issue Brief: China's Infrastructure Build-up in the Tibet Autonomous Region and along the Indian Border: What India Can Do" *Delhi Policy Group*, 2014, pp. 2–4.

6. Rajagopalan, Rajeswari Pillai and Prakash, Rahul "Sino-Indian Border Infrastructure: An Update", Occasional Paper No. 42, Observer Research Foundation, May 2013, pp. 6–10. http://www.orfonline.org/cms/sites/orfonline/

modules/occasionalpaper/attachments/Occasional42_1369136836914.pdf

7. Raheja, pp. 4–5.
8. Sudha Ramachandran, "India's Worrying Border Infrastructure Deficit," *The Diplomat*, (July 19, 2014). http://thediplomat.com/2014/06/indias-worrying-border-infrastructure-deficit/. **Editor:** Similarly, as seen from comparison of Google Earth satellite imagery between June 2011 and February 2013, China has also built the infrastructure for a modern surface to air missile base south of Hotan (和田), the closest major city to western border disputes, and home to an unidentified mechanized infantry division.
9. Rajagopalan, pp. 10–12.

***

Mapping China's Small Arms Trade: China's Illicit Domestic Gun Trade

By Zi Yang

This is part one of a two-part series examining China's arms trade.

China is one of the world's top small arms producers, and the products of official arms companies such as Norinco (北方工业) make regular appearances in conflicts around the globe. In 2014, Chinese arms and ammunition export totaled at $161 million, out of which sporting and hunting long guns constituted $12.75 million (UN Comtrade; NISAT). Despite the country's position as one of the world's largest arms producers, strict Chinese gun laws are designed to ensure few, if any, of its own citizens have the legal right to keep arms. Much less noticed is China's growing problem with domestic production of illegal firearms, which have helped fuel a recent spike in crime.

Even hunting, which is sanctioned on paper and, according to China's legal code should allow a limited number of guns for hunters, is curtailed, as licenses are no longer issued. Moreover, the penalties for gun ownership, and anyone caught involved in manufacturing, sales or ownership of guns can potentially receive a minimum of three years imprisonment. The crime can also carry a life sentence or the death penalty (Xining Public Security Bureau, July 27). **[1]** Despite these restrictions, Chinese police continue to discover and bust sizable gunrunning networks on a regular basis. A recent raid in Hunan's Shaodong province seized 1,180 guns, some 1,300 parts and 6 million rounds of ammunition—prompting the question, why, despite the tough gun laws in place, does China's illicit gun trade continue to flourish (People's Daily Online, November 28)? Judging by available evidence, China's expanding gun trade is a byproduct of its well-to-do population's growing demand for illegal goods. However, the existing ban, which makes legal gun purchases for law abiding citizens nearly impossible, has resulted in the disproportionate allocation of guns to criminal groups, adding new challenges to the maintenance of public and social order.

Identifying the Customers

Government intervention in the economy almost always has unintended consequences. High tariffs encourage smuggling, and bans on certain commodities creates black markets where products may still be traded. Similarly, China's underground gun trade is a result of the state's attempt to ensure its security by subduing market forces. But as long as a constant demand exists, there will be entrepreneurs willing to take risks in supplying the goods—and Chinese demand for guns is on the rise. Thus, the initial step to understanding China's illegal gun trade is analyzing the demand side.

Customers can be classified into two categories. The majority consists of players in China's criminal underground, the “black society” (黑社会), that straddle the line between the legal and illegal worlds—owners of massage parlors, coal mines, night clubs—and who must interact with career criminals on a regular basis. **[2]** According to a 2013 study, 63.2 percent of Shanghai’s inmates arrested on gun-related charges have previously been involved in drugs, illegal gambling, and prostitution. These individuals need guns mainly due to the high-risk nature of their work, and usually obtain guns from suppliers within their criminal circle. **[3]** Despite the restrictions on even the most basic of guns, some mobsters even have access to high-power weapons. One notorious example is Liu Han, a mobster and businessman in Sichuan Province closely associated with disgraced security czar Zhou Yongkang. To push through business deals, Liu frequently used a team of enforcers armed with military-grade weapons to intimidate and even murder his competitors (NetEase News Online, February 20, 2014; Sina News Online, April 24, 2014). **[4]**

Another type of customer who constitutes a significant minority is the general gun enthusiast, who has a legal occupation, but want to own a gun to satisfy personal interest, for hunting, or simply as a trophy. Generally coming from China’s rising middle-class and *nouveau riche*, these customers are growing and are known for their readiness to spend liberally for quality arms. **[5]**

Tracing the Supply Chain

The gun trade is a free market economy open to new entrepreneurs. The learning curve is moderate, but ultimately it is quite easy for anyone to join the commercial activities as long as he or she has the knowledge and proper connections. Before entering the industry, one must first acquire the relevant technical know-how. The traditional way of doing so is finding a gunsmith (枪匠). Police crackdowns on China’s traditional gun making hubs—Songtao County of Guizhou in particular—have forced gunsmiths with generations of passed-down expertise to leave for opportunities in the big cities. **[6]** Yet, finding people with such skills is hard because of the invisibility of this kind of labor market to most people. But in the digital age, joining the right Internet forums and QQ groups opens up a world of information that includes anonymous advice on anything gun-related, detailed gun blueprints, and scans of ordinance factory manuals that were considered secret just decades ago.

To be successful in the knowledge acquisition stage, one must first learn the language of the trade, i.e. the “black talk” (黑话). Dodging the Internet police is a part of Chinese online life and an argot was created to connect gun enthusiasts safely. Asking directly about guns (*qiang*) is too risky, so gun enthusiasts substituted *qiang* for *gou*, meaning dog in Chinese, as it is the homophone for the English word gun. Referring to one another as *gouyou* (狗友), literally “dog-buddies,” Chinese gun enthusiasts call assault rifles *chongfenggou* (lit. assault-dog), air guns *qigou* (lit. air-dog), shotguns *sandangou* (lit. loose-bullets-dog), handguns *shougou* (lit. hand-dog) and ammunition *gouliang*—dog food. **[7]**

For any business to operate, it must have goods in stock. Buying smuggled guns made outside of China is possible, but it is more cost-effective to manufacture locally. Most gun parts can be made without much difficulty. With a gun blueprint, an entrepreneur can easily replicate parts en masse at a hardware workshop or at home if they have the machinery. Some specialized parts and processes, such as barrels and riffling (cutting a spiral groove along the inside of a barrel to impart spin on a bullet) require less common tools. Barrels with rifling can only be purchased at specialty shops in certain parts of the country (mainly Guangdong) or online. **[8]**

Online hunting and military affair forums provide access to private QQ groups serving as virtual gun expos where sellers and buyers meet, network and trade. **[9]** Pricing is competitive, and sellers market their products by offering better prices and services. **[10]** Although scammers do exist, the majority are serious businessmen looking to make sales. Upon sealing a deal, the buyer would be directed to a *Taobao* (Chinese Ebay) store and pay for a legal product (*Hangzhou Daily*, March 1, 2013). The seller will then mail out disassembled parts of a gun in separate packages to the buyer. **[11]** Orders come with instructions on how to reassemble the gun, but the buyer may still contact the seller, or an after-sales service agent in the network for further assistance on reassembling, test firing, or returns and refunds. Once the buyer is satisfied, all record of sales will be erased. Despite the covert nature of the transactions, gun sales of all types continue to increase. As an examination of a recent case shows, the rewards for those willing to risk the law can be great—though the punishment if caught, even greater.

The Gun Trade in Action: the Case of the "Fang Lei Network"

At 38 years of age, Fang Lei is a millionaire in handcuffs. Originally a karaoke bar owner of Susong County, Anhui Province, Fang built an empire on running guns. A lifelong gun enthusiast, Fang described his attitude toward guns as like "women and make-up—cannot live without [them]." **[12]** According to Fang, he wanted to own a gun since he was a child. By 2009 he had already bought two, and quickly moved from collecting to selling. After joining the online "dog-buddies" community, Fang spent 24,000 Yuan (Ren Min Bi) on two rifles. He then began advertising a brand-new version of an AirForce Condor, the most popular brand of pre-charged pneumatic air rifle among Chinese hunters on Internet forums. Orders started flooding in immediately, and Fang had to travel to Guangdong's Foshan eight times in the following months to place orders for parts. Using barrels bought online, Fang assembled and sold the AirForce Condor air rifles, (which are just as illegal in China as assault weapons), at 7,000 Yuan each, making a 5,000 Yuan profit per transaction. As business boomed, Fang recruited more workers into his network. By the time of his arrest, his QQ group "Comma Family" had more than 300 members. To maintain security, they agreed to never video chat with one another or meet in person. Ultimately, Fang constructed an underground business empire, with him at the pinnacle, directing hundreds of sales agents across the country. According to police records, Fang's network made at least 784 successful transactions before his arrest in 2012. **[13]** In the scheme of China's underground gun manufacturing networks, the dismantling of the Fang Lei Network meant little. There are still thousands of similar organizations in China's prospering illicit gun trade.

Conclusion

China's expanding underground gun trade is the byproduct of the state's struggle with market forces. The state fears an armed populace, but a strict ban on gun ownership has only created a black market where the wealthy and well-connected can still buy guns with ease. With the growth of the Chinese economy, the gun trade will continue to expand in response to rising demand from a population with money to spend and an appreciation for weapons stemming from its culture and history. Currently, the gun ban is unlikely to be lifted, yet it is necessary for the Chinese state to recognize the unintended consequences of the ban, and how it allocates guns disproportionately into the hands of black society syndicates that constitute a threat to the livelihood of law abiding citizens, a phenomenon that will have long-lasting negative consequences for social stability.

Zi Yang is a graduate student at Georgetown University School of Foreign Service. He currently serves as a research assistant at Georgetown University's Center for Security Studies.

Notes

1. Yang Jiang 杨江, 黑枪调查 [Investigating Illicit Guns], *Xinmin Weekly* 44 (November 2012): 54.

2. Chen Junwu 陈君武, Zheng Yonghong 郑永红 and Zhang Hongmei 张红梅, 我国非法制贩枪支犯罪的发展态势及对策 [The Trajectory of Our Country's Manufacturing and Sales of Illicit Guns and Proposals for Countermeasure], *Journal of Chinese People's Public Security University (Social Sciences Edition)* 5 (October 2011): 35; Wu Xingmin 吴兴民, 广东涉枪犯罪的特点及治理对策思考 [On Characteristics Of Gun-related Crimes in Guangdong and Countermeasures], *Journal of Henan Police College* 3 (June 2012): 22.

3. Pang Yan 庞岩, 涉枪犯罪的调查研究 [A Study on Gun-related Crime], *Guangdong Public Security Technology* 3 (September 2013): 16–17.

4. Collaboration between black society bosses and Communist Party officials is nothing new in China. The anti-corruption campaign, in fact, has unmasked many cases of such nature. For a recent reportage on a cabal of Shanxi officials, criminal syndicates and businessmen, see: QQ News Online, November 12.

5. Zhang Dezhi 张德智, 当前涉枪犯罪案件的特点及侦查对策 [Characteristics and Investigation Countermeasures of Current Gun-related Crime Cases], *Journal of Liaoning Police Academy* 3 (May 2012): 25; Pang Yan 16–17.

6. Chen Junwu, Zheng Yonghong and Zhang Hongmei, 31.

7. Yang Jiang, 53; The term *gouyou* has a meaning equivalent to American slang "dawg."

8. Customs inspection in China is weak. Shenzhen's Huanggang, the country's largest port of entry only has the capacity to fully inspect two percent of the daily 20,000 incoming and outgoing vehicles. See: Cao Yunqing 曹云清, 走私犯罪的现状与发展趋势 [Smuggling-related Crime and its Future Trajectory], *Journal of Jiangxi Police Institute* 6 (November 2014): 30.

9. Li Min 李民 and Gao Fengli 高凤立, 必要帮助犯之主犯化——以网络涉枪犯罪中提供“交易平台”和“技术信息”为例 [From Abettor to Prime Culprit—A Study of the Internet's Role in Providing a "Trading Platform" and "Technological Information" for Gun-related Crime], *Journal of Dalian Maritime University (Social Science Edition)* 3 (June 2015): 81.

10. Yang Jiang, 54–55.

11. Some larger networks follow a more intricate procedure by mailing parts to different addresses around the buyer's locality. Once delivered, the buyer may choose to personally pick-up the parts or receive drop-offs from sales agents.

12. Wang Jiangen 王健根 and Xie Lei 谢磊, "谁在贩枪?" [Who is Running Guns?], *People's Police* 23 (December 2012):12.

13. According to Chinese law, a gun is defined as having the muzzle energy of 1.8 joules per cm^2 or more. In practical terms this translates to the ability of gun's projectile to penetrate an aluminum soda can. This also means trafficking pre-charged pneumatic air rifles carries the same legal consequences as trafficking firearms. See: Ministry of Public Security, March 22, 2011.

*** *** ****