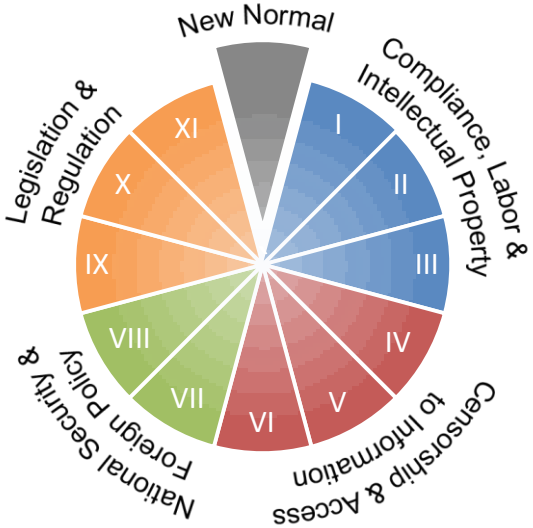
U.S. Department of State
Overseas Security Advisory Council

# XI Ways Xi is Changing Chinese Security

## November 2015

# XI Ways Xi is Changing Chinese Security




*Executive Summary*

### The New Normal

After decades of double-digit growth, the Chinese economy is showing signs of much more modest performance. Wary of the implications of this slowdown on social stability, the Communist Party of China, led by President Xi Jinping, appears to be heightening measures to consolidate control and minimize any threats to its authority. While suggestions that the Party is facing an existential crisis may be premature, the terms and conditions of operating in China are likely to become more difficult for the private sector.

### Compliance, Labor, & Intellectual Property

I. The Communist Party and the private sector are both targeting corruption – but for different reasons – complicating the ability to conduct due diligence.

II. Companies looking to scale back their operations should prepare contingency scenarios, as authorities may be reluctant to arbitrate in their favor.

III. Threats to intellectual property are unlikely to disappear and could get worse as the country moves toward “innovation” as a driver of the economy.

### Censorship & Access to Information

IV. The list of subjects that are off-limits in China appears to be growing, with hundreds of journalist detained already this year.

V. Use of social media has been further restricted, as it may represent one of the most likely sources of collective resistance.

VI. Lack of objective and comprehensive reporting will increasingly challenge the private sector’s ability to make real-time safety and security decisions.

### National Security & Foreign Policy

VII. A year long “crackdown on terrorism” has done little to resolve the root causes of extremism in China and may actually exacerbate tensions.

VIII. The real value of disputed maritime claims may be the *conditional* political capital derived from leveraging nationalist sentiment.

### Legislation & Regulation

IX. “Rule of law” efforts may be more interested in consolidating and codifying authority than establishing a transparent legal framework.

X. New laws may be used to increase pressure on foreign NGOs, whose influence is perceived to be a threat to the Communist Party.

XI. Legislation could emphasize “national security” as a pretext to bolster domestic industry.

# A "new normal" for China

China has achieved one of the most remarkable periods of sustained economic development in history. From 1978 to 2013, the economy grew at an average annual rate of nearly 10 percent, doubling in GDP every eight years and lifting more than 400 million people out of poverty. This reliable economic performance and consistent improvement in the Chinese quality of life became a pillar of legitimacy for the Chinese Communist Party, which has ruled the country uncontested since 1949.

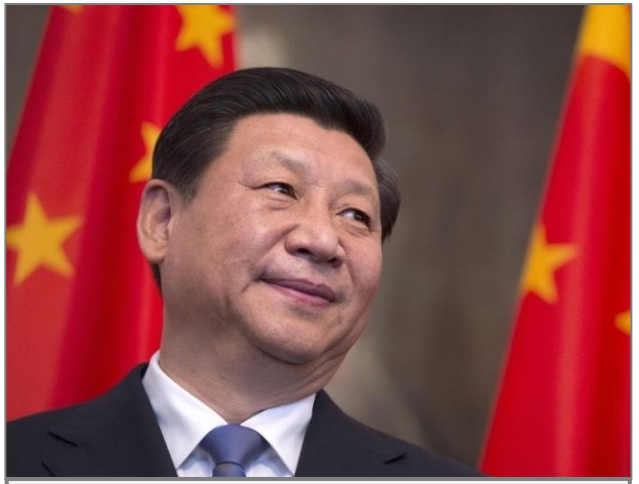
Recent figures, however, suggest China is now entering a chapter of more modest development. Though still impressive in absolute terms, last year's growth rate of 7.4 percent was the lowest in nearly a quarter century. Policymakers are faced with the tough task of implementing difficult economic reforms – which could lead to even further declines – while still meeting self-imposed growth targets. This challenge is compounded by increasing income inequality, environmental degradation, an aging workforce, and mounting debt.

The economic slowdown (or "new normal" as it is referred to by Beijing) has coincided with the ascension of President Xi Jinping. Drawing on lessons from the Soviet Union's experiments with social and political reform in the late 1980s, and its subsequent collapse, Xi appears concerned about threats to the party and anxious to reassert control. This retrenchment is evidenced by a sweeping campaign against corruption, an increasingly restrictive censorship regime, an assertive domestic security and foreign policy posture, and a host of opaque and evolving security laws.

Fortunately for the U.S. private sector, these trends do not necessarily indicate that the Party is facing an existential crisis or that massive political unrest is imminent – notions of the Party's "inevitable" collapse have been around for decades but the Party has proven remarkably resilient. Nor should the evolving security environment necessarily deter private sector organizations from entering China or cause those with existing operations to reconsider their presence.

The terms and conditions of operating in China, however, are changing. Even if it remains too early to determine President Xi's ultimate impact on the private sector, risk managers and intelligence analysts who take a more holistic view of security – incorporating issues like rule of law, access to information, nationalism, due diligence, and labor – may be better equipped to address a number of potential challenges on the horizon.


*Source: World Bank*



Xi Jinping

President of China, 2013 -

# I. Anti-corruption campaign highlights due diligence challenges

One of the hallmarks of Xi's presidency has been his campaign against corruption. Hundreds of thousands of Party members have already been investigated for "extravagance, formalism, and bureaucratism," a euphemism for graft, with over 70,000 punished in 2014 alone. While a majority of these cases involves officials at the local or municipal levels, at least 80 current or former senior officials – commonly referred to in China as "tigers" – have been punished since Xi come to power. As to *why*, it is unlikely that Xi's campaign against corruption can be reduced to a singular motive. A better explanation is that it accomplishes a number of strategic goals, such as restoring public faith in the integrity of the Party; targeting prospective challengers within the Party; and improving the efficiency of government, state-owned enterprises (SOEs), and the military.

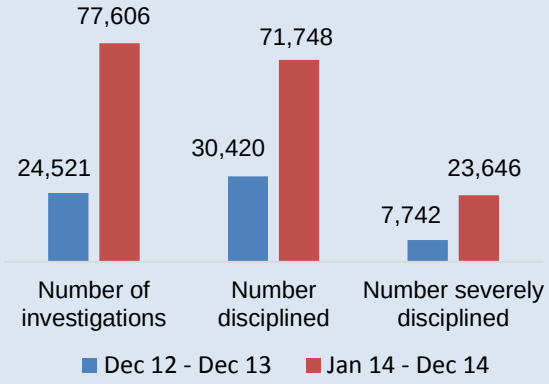
The first lesson for the U.S. private sector is that Xi's campaign highlights the prevalence of corruption in China. Though much of the ill-gotten wealth of those who have been investigated may have come from SOEs, confiscation and resale of land, or embezzlement, corruption continues to adversely impact the U.S. private sector as well. Organizations operating in China are encouraged to conduct due diligence to ensure the integrity of any potential business ventures and to be wary of individuals or enterprises who may expect bribes.

The second lesson may be a somewhat ironic derivative of the first. Regardless of the motives of the anti-graft effort, it seems to be tightly controlled. President Xi and his powerful anti-corruption czar, Wang Qishan, do not appear to need or to want help from outsiders; on the contrary, Xi and Wang may be wary of unsanctioned investigations that identify too much too fast or that condemn the *wrong* people. As a result, while the Party and the private sector are both attempting to identify instances of corruption, the targeted nature of the former may complicate the ability of the latter.

To tighten its grip on the anti-corruption campaign, Beijing has implemented new rules restricting access to company records at local industry and commerce bureaus – information which had previously allowed compliance teams and due diligence investigators to vet potential business partners on the grounds of corruption or malpractice. Such information can be particularly valuable in China, where millions of individuals share the same surname, company documents are relatively easy to manufacture, and official records are often kept close hold. Those who trade in this information run the risk of being charged with "selling or unlawfully transferring personal information," as was the case with a British investigator who recently spent nearly two years in a Chinese prison.

Non-transparent rules regarding personal information make it difficult to provide explicit guidance. When in doubt, the private sector is encouraged to work through local experts who speak the language, understand the legal environment, and are better equipped to avoid the pitfalls of potentially compromising due diligence investigations.

**Corruption investigations on the rise**




*Source: Foreign Policy*

**Notable Senior Officials ("Tigers")**

**Zhou Yongkang**
*Sec. of Central Political & Legal Affairs Commission*

**Bo Xilai**
*Secretary of Communist Party for Chongqing*

**Ling Jihua**
*Principal Advisor to Former President Hu Jintao*

**Su Shulin**
*Incumbent Governor, Fujian Province*

# II. Economic slowdown presents labor challenges

One of the principal drivers of China's current economic slowdown has been a shrinking of the country's labor-intensive manufacturing sector. This has resulted in an increasing number of strikes by Chinese workers, who may be dissatisfied with deteriorating conditions, reduced wages, and job losses. According to Hong Kong-based *China Labour Bulletin*, this rising strike activity not only disrupts operations, but is often met with police intervention – some of which can turn violent. In the case of state-run factories, the principal risk is often that incurred by the demonstrators and labor organizers themselves; concerns of broader public disorder or collateral violence are typically limited due to swift state security intervention.

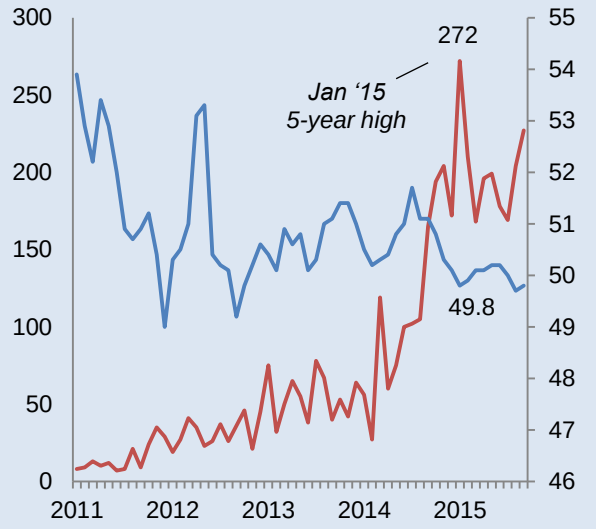
That is not necessarily the case when it comes to the foreign private sector. A number of Western firms have trimmed operations in China due to more moderate economic forecasts, workforce automation, and rising labor costs. In a number of instances, these cutbacks have resulted not only protracted stoppages, but also the temporary detention of expatriate managers by workers demanding continued employment or enhanced severance packages. Chinese authorities, wary of both lost tax revenue and public discontent stemming from job loss, have been reluctant to intervene and arbitrate in favor of non-Chinese employers. Authorities' justification for not responding – in spite of these seemingly aggressive tactics – is that the incidents are "business disputes," rather than state security matters.

That does not necessarily suggest that companies are "stuck" in China. To mitigate the potential risk of harassment, detention, or confiscation of machinery and goods, private sector organizations should approach the issue of workforce reduction holistically, incorporating their legal, human resources, *and* security teams. According to one risk management specialist, this involves "identifying all of the stakeholders who would be affected by restructuring and understanding their needs and motivations." That can mean working with local interlocutors to understand grievances and expectations for fair compensation, and then communicating company policies in a way that is acceptable to and understood by all employees.

As for specific security considerations, private sector organizations may coordinate with local law enforcement authorities, keep security personnel on hand when restructuring announcements are made, and limit access to – and therefore vulnerability of – expatriate managers. While this may not eliminate the challenges of reducing an organization's workforce, anticipating and addressing potential security issues before they occur is likely to prove easier than resolving them after the fact. Additionally, this may serve to minimize negative press, especially as the Chinese public becomes increasingly active online, using social media in a way that can damage an organization's reputation when their demands are not met.

**Strikes increase as manufacturing decreases**

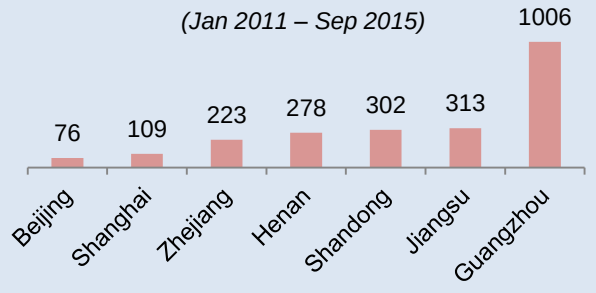
*(Jan 2011 – Sep 2015)*




*Sources: China Labor Bulletin, Caixin/Markit Purchasing Market Index (PMI)*

**Total number of strikes in China by location**

*(Jan 2011 – Sep 2015)*




*Source: China Labor Bulletin*

# III. Threats to information security unlikely to abate

Last May, the U.S. Department of Justice made history when it formally filed charges against five Chinese military hackers for economic espionage directed against U.S. private sector organizations. This year, comments from U.S. authorities suggested that a cybersecurity breach of the U.S. Office of Personnel Management (OPM), one of the largest of its kind in history, may have been perpetrated by Chinese actors. Although these incidents received considerable media coverage, they are only the most newsworthy of a much broader trend. According to the *IP Commission Report*, more than 80% of all information theft attempts targeting Americans may come from China.

There was measured optimism this September, when a visit to Washington by President Xi yielded an agreement that China and the U.S. would refrain from attacks aimed at stealing private sector intellectual property (IP) for commercial advantage. Even before Xi's trip to the U.S., Beijing reportedly arrested a number of hackers at the behest of U.S. authorities, possibly to signal a tougher stance against hacking.

Despite these symbolic gestures, experts suggest threats to IP are unlikely to disappear any time soon. This doubt stems in part from the lack of universally agreed upon definitions of "trade secrets" or "commercial advantage," and the absence of metrics for measuring compliance. Moreover, demonstrating attribution has always proven difficult and there are concerns that a directive not to target IP may only lead to the use of third parties, or "proxies," who would give authorities plausible deniability. Conversely, the incentives for stealing IP may actually *increase* as Beijing redoubles investment in the information and communication technology sector, for whom cutting edge trade secrets represent a means of closing the innovation gap and bolstering Chinese national firms.

Although IP theft can occur anywhere, even without a physical presence, the threat may be even more acute for individuals traveling to or operating in mainland China. As the OSAC Beijing Crime and Safety Report notes, visitors to China should have no expectations of privacy. Taxis, hotel rooms, and meeting spaces are all subject to on-site and remote technical monitoring. Furthermore, the Chinese government's access to infrastructure means that all forms of communication, including phone calls, faxes, e-mails, and text messages, as well as Internet browsing history, are likely monitored.

Any vulnerabilities that are exposed while visiting China not only affect the individual traveler and the information contained on his/her device, but may also serve as an entry point into an organization's secured network. Upon successful intrusion, threat actors may enjoy continued network access long after the traveler has departed, facilitating the theft not only of trade secrets (e.g., formulas, designs, and chemical compounds), but of any information that would give an organization a competitive advantage (e.g., contacts, finances, and business models). To mitigate this threat, security managers can begin by educating employees on the frequency and financial impact of IP theft, offering clean "loaner" devices for short-term travel, and providing an overview of common threat vectors like spear phishing and social engineering (see callout for more tips).

**Best Practices for Traveling to China with Mobile Devices**

***BEFORE***

- ❑ Leave all non-essential devices at home
- ❑ Provide clean "loaner" devices without proprietary information or stored passwords
- ❑ Back up all important data
- ❑ Strengthen passwords
- ❑ Update software and apps (to patch any bugs or vulnerabilities)
- ❑ Delete sensitive information
- ❑ Enable firewalls
- ❑ Disable Bluetooth and GPS
- ❑ Do not announce planned trips, itineraries, whereabouts, etc. on social media

***DURING***

- ❑ Maintain physical control of devices at all times
- ❑ Do not sign on to public Wi-Fi networks
- ❑ Do not click links in email and text messages from untrusted senders/domains
- ❑ Terminate connections after Wi-Fi use
- ❑ Use a Virtual Private Network (VPN)

***AFTER***

- ❑ Avoid immediately connecting mobile devices to personal or business networks
- ❑ Scan devices for malware independently or with the help of your IT department
- ❑ Change all passwords

# IV. The list of unspeakable subjects may be growing

For decades taboo topics in China were thought of as the three T's: Tibet, Taiwan, and Tiananmen. There have also been one-off events that triggered a severe clampdown on press freedoms, such as the 2003 SARS outbreak, the 2008 Sichuan earthquake, and a 2011 high-speed train wreck. As one scholar notes, however, the boundaries of what subjects are permitted are always in flux, and they appear to have narrowed since President Xi came to power.

New laws were announced in June 2014 that, according to official Chinese media, "cover various information, materials and news products that journalists may deal with during their work, including state secrets, commercial secrets, and unpublicized information." Whereas journalists may have previously been able to report somewhat objectively on major incidents, so long as they did not criticize official response, authorities under Xi appear anxious to suppress *all* reporting of sensitive issues, regardless of the author's position. Although the callout provides a few recent examples of sensitive topics, it may be less important to know *which* subjects are off-limits, and more important to consider *why* they are off-limits. Generally speaking, anything that questions the effectiveness of government policies or provides an alternative narrative than that which is put forth by Beijing may be censored.

When the sinking of a cruise ship on the Yangtze river in June left over 440 people dead, President Xi reportedly imposed roadblocks more than one mile from the incident to prevent any unsanctioned coverage. Even relatives posting requests for information about the status of missing loved ones had their messages blocked. This August, nearly 200 Chinese journalists were punished for their role in reporting on the depreciation of the stock market, the Tianjin explosions, and the WWII anniversary celebrations. Although some may have been guilty of hyperbole or speculation, their crime, according to official Chinese media, was that they, "caused panic, misled the public, and resulted in disorders in stock market or society."

For security managers, restrictions on what commentary is permissible can have direct implications for the health and safety of the individuals they are employed to protect. Punitive measures for those who violate strict editorial guidelines are not confined to dismissals, libel lawsuits, and fines, but have increasingly included arrests and forced televised confessions. According to the Committee to the Protect Journalists, last year China jailed more members of the press than any other country, a majority of whom were held on "anti-state" charges.

Censorship is not limited to journalists reporting from within China, but includes increasing restrictions on information emanating from outside the country's borders as well. Foreign media organizations that report on sensitive issues in China may be blocked altogether, as has been the case with *New York Times*, *BBC, Bloomberg,* and others. Chinese censors may also proactively preempt foreign journalists from reporting on politically sensitive topics by denying them visas. Addressing this idea at a press conference last year, President Xi reportedly cited a Chinese parable that says, "Let he who tied the bell on the tiger take it off," which can also be translated as "the one who created the problem [in this case the foreign journalists] should be the one who solves it…"

**Topics resulting in sites being blocked or journalists being detained**

- Exposés on the wealth of senior Party members and their families
- The regions of Tibet and Xinjiang (generally)
- Sensitive social issues (e.g., pollution, forced land acquisition, and HIV/AIDS)
- Political dissidents (e.g., Dalai Lama, Liu Xiabo, Cheng Guangcheng)
- Government disaster response (e.g., the 2003 SARS epidemic, the 2008 Sichuan earthquake, and the 2015 Tianjin explosions)
- Ideas that could erode market confidence or weaken the economy (e.g., official handing of the 2015 stock market downturn)


*In August, Wang Xiaolu, an influential reporter for the financial magazine* Caijing *was forced to give a televised confession in which he admitted to using "private information obtained through inappropriate channels," exercising "subjective judgment," and "seeking to create a sensation," following a story that suggested a Chinese securities regulator was attempting to prop up falling stock prices.*

# V. Social media as a source of political change

While the previous section considered the anxiety stemming from the *criticism* of Chinese officials or Party policy, President Xi's enhanced efforts to control the conversation online may belie an even greater concern – the Internet and social media as a source of unified resistance. Having witnessed the Arab Spring and the Occupy movements, in which social media was integral to galvanizing dissent and, in some cases, enacting political change, authorities appear increasingly determined to prevent the Internet from becoming a source of mobilization.

Much of the staying power of the Communist Party is rooted in its size and singularity. With 90 million members, the Party may be willing to reluctantly endure some modest groveling about government services, so long as the author has limited influence. What the Party appears unequivocally opposed to, however, is the emergence of an activist or public personality who could bring together popular resentment and demand a political alternative.

China now has roughly 668 million Internet users (or more than twice the entire population of the U.S.), each of which presents a potential source of dissent. In order to control political discourse, the Party relies on a massive domestic security apparatus. Although much of the censorship is automated, official state media has suggested that up to two million Chinese are employed to scrub derogatory blog plots, filter sensitive keyword searches, and shut down controversial websites.

Under President Xi, Internet censorship appears to be getting even worse. In 2013, Beijing enacted a law in which individuals "fabricating facts to slander others" online could be held up to three years in prison if the author had at least 5,000 followers or if the comments were reposted 500 times. This November, official Chinese media announced that the punishment had been extended to *seven* years. In October, Freedom House's Freedom on the Net 2015 report ranked China as the *worst* abuser of Internet freedom in the word, citing its "attitude toward foreign Internet companies, its undermining of digital security protocols, and its ongoing erosion of users rights."

Chinese authorities are not the only ones responsible for controlling the conversation online. The pending Cybersecurity Law reinforces preexisting conditions that all network providers operating in China (including foreign firms) require users to register using their real names – ostensibly to preempt anonymity and increase accountability. These same firms are also explicitly made responsible for immediately deleting any information prohibited by the law, for preventing the spread of such information, and for reporting infractions to the relevant authorities. Organizations that are unwilling or unable to adhere to these terms may be forced out of China and replaced by more compliant domestic alternatives.

Even for those who are not in the IT industry, online censorship can have an impact on how employees use the Internet in their daily work lives. Examples include students using search engines to conduct research or global employees using online collaboration platforms. Travelers to China should note that not all foreign websites, social media platforms, and email services are accessible and should plan correspondence options accordingly.

### Internet Services… Made in China

Rather than attempt to hamper foreign influence exclusively through blocking external content, Chinese authorities have recognized the insatiable demand for online commerce and communication and have facilitated the development of domestic alternatives to their popular Western counterparts.

*Baidu*, perhaps best understood as the Chinese version of Google, is primarily a search engine that boasts of dozens of other online services including maps, cloud storage, and an encyclopedia. While its usage as a search engine lags behind that of its Western counterparts, Baidu consistently ranks as the fourth-most popular website in the world.

*Alibaba* is an online commerce conglomerate whose 2014 sales were greater than those of Amazon and eBay *combined*. During its U.S. IPO last September, it raised USD 25 billion, more than any company in history.

*Tencent* is an online media, entertainment, and social media group, perhaps best known for its QQ instant communicator and "WeChat," the most popular app in China. In September it surpassed Alibaba as the most valuable tech company in Asia, with market cap of over USD 200 billion.

# VI. Absence of available information impedes decision-making

Perhaps the greatest impact of Chinese censorship on the U.S. private sector is the inability to access comprehensive and transparent information, particularly in the wake of important security developments.

In August, two explosions rocked the Chinese port city of Tianjin. Shortly after, it was revealed that the warehouse that had exploded housed 700 tons of sodium cyanide and other hazardous materials. Officials commented that the possibility of long-term health implications was limited outside the immediate blast zone, but denied journalists and environmental groups access to the site to conduct their own independent assessments.

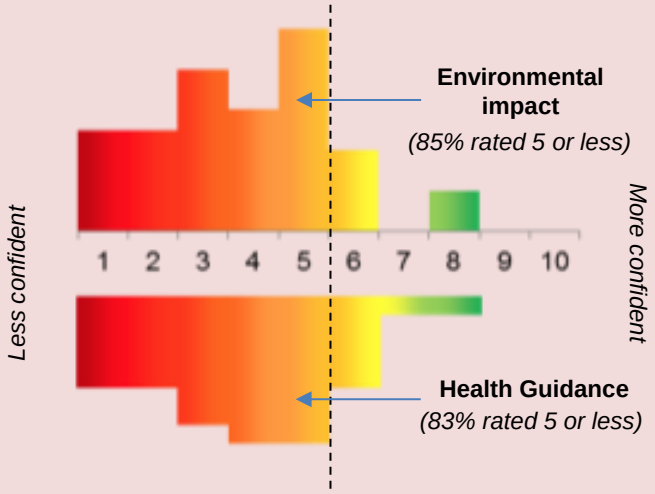
Just six weeks later, 18 parcel bombs exploded in China's southern Guangxi province, killing 10 people and injuring more than 50. Chinese authorities immediately discounted the possibility of terrorism and pinned the seemingly complex attack on an aggrieved quarry worker. If there were more to the story, such as the political motives of the perpetrator or accomplices, it was not revealed in scarce official media reporting.

In both of these instances, U.S. private sector security managers expressed concern about the scarcity and subjectivity of Chinese media reporting. An absence of objective, independent information, many suggested, complicated their ability to make informed decisions about the future health and safety of their employees and forced them to choose between imposing restrictions out of an abundance of caution, or proceeding with operations despite serious reservations. Those observations align with broader concerns expressed by U.S. private sector organizations operating in China. According to American Chamber of Commerce Beijing's 2015 China Business Climate Survey, 83 percent of respondents suggested that Internet censorship negatively impacts their ability to conduct business in China.

Security managers may moderate this lack of information by understanding the nature of allowable media (even if it is not necessarily transparent and inclusive) and the biases that may be built into official Chinese media outlets. Organizations may also identify what Virtual Private Networks (VPNs) exist, as they could potentially present a means of circumventing restrictions on access to information. Finally, private sector security managers are strongly encouraged to participate in information sharing networks, such as OSAC Country Councils and American Chambers of Commerce, as a means to benchmark their experiences and observations with industry peers.

**Limited Confidence in Official Media Report**

*In the aftermath of the August 2015 Tianjin explosions, OSAC constituents were asked to rate their confidence in official reporting on the following (on a scale of 1 to 10):*




*Source: OSAC August 2015 Tianjin Impact Survey*

# VII. Counterterrorism tactics may actually fuel resentment

China's northwestern Xinjiang region routinely experiences violent clashes between Chinese security forces and the predominantly Muslim Uighur minority. In public statements, government officials broadly characterize all Uighur discontent as terrorist activity and single out the "Three Evils" of extremism, separatism, and terrorism in Xinjiang as the main terrorist threat to the nation.

Although the inter-ethnic tensions at the root of these clashes can be traced back several decades, President Xi's tenure has witnessed an increase in both the scale and scope of attacks attributed to Uighur militancy. No longer confined to the remote Xinjiang region, recent years have seen attacks as far east as Kunming and Beijing. In addition to knives, which assailants typically use due to strict gun control laws, Uighur militants have increasingly used vehicles and crude explosive devices to conduct indiscriminate attacks against civilians at public venues like outdoor markets and train stations.

Following a series of particularly violent attacks last spring, in which nearly 80 people were killed over a three month period, Chinese officials announced a year-long counterterrorism campaign aimed at restoring stability and resolving communal tensions. This involved not only augmenting security personnel and intensifying surveillance, but also introducing measures that appear intent on forging a unified Chinese identity. These included banning Uighur men from wearing beards or women from wearing veils; barring Uighur women, children, and officials from attending mosque; and prohibiting Uighurs from fasting during Ramadan.

It is difficult to know if the campaign against counterterrorism has been successful. Authorities have apparently clamped down on press coverage in the region, ostensibly because news of attacks could both exacerbate communal tensions, as well as undermine propaganda efforts regarding the success of the campaign. In one recent example, the massacre of 50 miners in Xinjiang was reported in mainstream U.S. media, but was not acknowledged by Chinese officials, despite a reportedly massive manhunt for the assailants. More recently, the Communist Party announced it had ousted the former editor of the *Xinjiang Daily* (notably, an ethnic *Han*) for publicly questioning official policy in the region.

Despite incomplete reporting, it is plausible that any temporary "peace" achieved at the expense of repressing cultural and religious identity could further fuel Uighur resentment and heighten the long-term potential for extremism. Additionally, pre-existing tensions could be amplified by pending investment that could see massive infrastructure projects in Xinjiang (potentially ushering in more Han workers and displacing local communities) and by the potential return of the roughly 300 Uighurs that Beijing claims to be in Syria.

For security managers, terrorism in China may remain a relatively modest security concern, as attacks have historically been directed against host-nation security forces in areas with limited private sector presence. However, the willingness to incur collateral casualties and demonstrated ability to conduct attacks outside of Xinjiang, coupled with repressive measures that exacerbate communal tensions, could signal a growing risk.


**Oct '13**, (Beijing), A vehicle careens through Tiananmen Square and explodes, killing two, and injuring 38 others. It marks Beijing's worst terrorist attack in a decade.

**Mar '14,** (Kunming, Yunnan) Thirty-nine people are killed when knife-wielding assailants indiscriminately stab civilians at a Kunming train station.

**Apr '14**, (Urumqi, Xinjiang) An explosion occurs at Xinjiang's largest train station, killing three people and injuring 79. The blast coincides with a visit by President Xi focusing on counterterrorism efforts.

**May '14**, (Urumqi, Xinjiang) An attack at an open air market in the restive northwestern region's capital using vehicles and explosives kills 31 people.

**Jun '14**, (Elixku, Xinjiang), nearly 100 people die when, according to Chinese reporting, 59 knife-wielding Uighurs storm a police station.

**Feb '15,** (Hotan, Xinjiang) eight people are killed and another seven injured when a suicide bomber detonates an explosive device in southwestern Xinjiang.

**Jun '15,** (Kashgar, Xinjiang) 18 people are killed when assailants attack police with knives and bombs at a security checkpoint, days after Chinese officials ban religious practices during Ramadan.

# VIII. Territorial disputes offer *conditional* political capital

Although disputes over territories in the East and South China Seas predate President Xi, Beijing's foreign policy posture in the region appears to have grown more assertive under the current administration. This includes the declaration of an Air Defense Identification Zone (ADIZ) over the Senkaku/Diaoyu islands (also claimed by Japan) in 2013; the placement of an oil rig off the coast of Vietnam in May 2014; and land reclamation projects in the South China Seas that have included the construction of runways, lighthouses, and military garrisons.

Beijing maintains that its sovereignty over these disputed territories is legitimized by historical claims dating back more than half a century. As for the purpose of exploration and construction, the Party cites not only military defense, but civilian demands including maritime search and rescue, safety of navigation, etc.

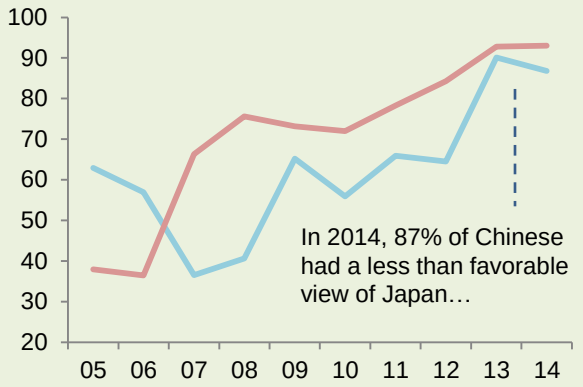
In addition to these security and commercial functions, the Party may increasingly highlight its territorial sovereignty as a "core national security interest" to satisfy a domestic imperative – that of growing Chinese nationalism. Following what Beijing refers to as a "Century of Humiliation" (from the 1839 Opium War until the end of Japanese occupation), expanding global influence and a patriotic education campaign appear to have fostered increasingly nationalistic sentiment. This may result in a Chinese public less inclined to accept prevailing international norms or historical balance-of-power relationships.

While some fear that nationalism could lead Beijing into a confrontation over disputed maritime claims, public sentiment may not be as reckless as is often depicted. In a recent survey, a majority of Chinese participants agreed unequivocally that Beijing's maritime claims were legitimate. However, when weighing possible options, less than half of the participants supported armed conflict and even fewer encouraged such a confrontation if it could potentially have a negative economic impact.

For its part, Beijing likely understands that while nationalist sentiment may bolster Party legitimacy, it can also present vulnerabilities. Too much domestic pressure might compel Beijing into a conflict in which an absolute victory would be difficult to achieve. Furthermore, demonstrations against foreign governments or militaries have the potential of creating instability or evolving into movements against the Party itself (especially if Beijing's response to foreign aggression is seen as weak or inadequate).

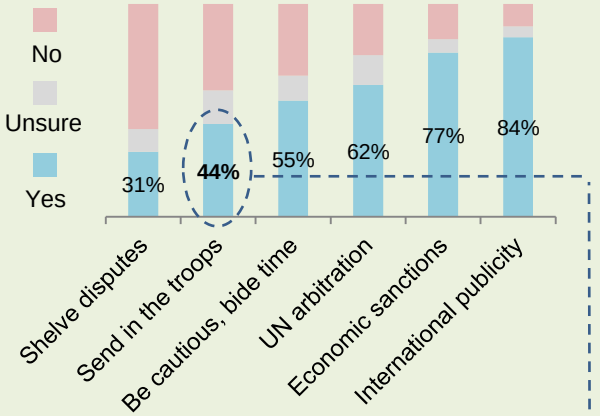
As a result, bellicose rhetoric and saber rattling is likely to continue on the surface, while a more cautious and pragmatic undercurrent moderates nationalist sentiment and actively seeks to avoid any potentially destabilizing actions. Public sentiment could lead to anti-U.S. or anti-claimant demonstrations, as was the case with anti-Japanese protests in China in 2012, and this bears monitoring. However, authorities are likely to limit any unrest that could jeopardize stability and hamper already modest growth forecasts.

**Sino-Japanese public perception**




*Source: Genron NPO*

**Chinese support of maritime dispute policy options**




…but less than half of Chinese surveyed in a recent poll supported the use of military force.

*Source: Perth USAsia Center*

# IX. "Rule of law" more about control than transparency

Clearly defined laws are crucial to the private sector; they provide a legal framework for what is permissible, identify the authorities responsible for enforcement, and outline the consequences of non-compliance. In China, however, Beijing has historically favored a more ambiguous set of rules and regulations that can be applied selectively and in accordance with the needs of the Party.

Beginning last October, President Xi underscored China's commitment to "advance the rule of law" – a term generally used to describe a nation that is governed by a transparent legal system, rather than by arbitrary enforcement of individual authorities or political parties. In the ensuing months, the country's legislative assembly put forth a wave of new security legislation, including the National Security Law (which passed in July) and the draft Cybersecurity, Foreign NGO Management, and Counter Terrorism laws.

Rather than clarifying ambiguities or providing legal assurances, however, these new laws appear more intent on broadening how Beijing defines security and entrenching the centrality of the Party. Of the National Security Law, for example, the *New York Times* suggests it is "a more abstract statement of principles, aimed at exhorting all Chinese citizens and agencies to be vigilant about threats to the Party."

In many instances, the laws appear to have been left intentionally vague, enhancing the authority of the Party to uphold national security and stability, while also granting it more room to maneuver on whatever social, economic, or political challenges it may confront. Some experts have said that the new laws "will give security agencies stronger legal footing in curbing perceived threats from social activists and government critics." Others worry that "enhancing the power of police and other government authorities, without additional revisions to ensure proper use of the law, will severely restrict the fundamental rights and freedoms of the people."

Journalists have pointed to the detention of dozens of Chinese lawyers in the weeks following the passage of the National Security Law as evidence that Beijing's commitment to "rule of law" may still remain largely rhetorical. The arrest, interrogation, and vilification of the very individuals who should have benefited from increased legal protections, they suggest, is evidence that law in China remains subordinate to the Party and not the other way around.

With respect to private sector impact, three of the bills still remain in draft form and it is uncertain how much they will be changed following public comment and private conversations (though optimism is measured). Even in their final format, it is unclear how aggressively these laws will be enforced, further challenging the private sector's ability to adequately anticipate their ultimate bearing. Broadly speaking, the new laws reflect a Communist Party that has grown anxious about threats to its legitimacy and is broadening its toolkit to limit their influence.

**What's on the books?**

*(translations by China Law Translate)*

- National Security Law
  (passed July 2015)
- Cyber Security Law
  (draft published July 2015)
- Foreign NGO Management Law
  (draft published May 2015)
- Counterterrorism Law
  (draft published November 2014)

# X. Fear of foreign influence places strain on NGOs

Recent legislation appears to suggest Beijing's growing apprehension with ideological or reformist threats posed by foreign governments, business, and civil society organizations. Article 15 of the National Security Law, for example, provides that the state "guards against, stops, and lawfully punishes acts of infiltration, destruction, subversion or separatism by *foreign influences*." Article 23 speaks of the "excellent traditional culture of the Chinese people" and the state's role in "*resisting negative cultural influences*."

The anxiety regarding foreign influence is perhaps most broadly revealed in the draft Foreign NGO Management Law, submitted for public review in May. According to the authors, the legislation is meant to safeguard the rights of NGOs and "promote cooperation and exchanges." But while granting foreign NGOs legal status might otherwise be a welcomed development, certain provisions have worrying implications.

As with other laws, the Foreign NGO Management Law seems to have been left intentionally vague, to expand the writ of the Party while granting it greater flexibility with enforcement. Foreign NGOs are defined as "any not-for-profit, non-governmental social organization formed outside of China." This means that the law not only applies to NGOs operating in more sensitive fields – such as human rights, labor, and religion – but to those dealing with "economics, education, science and technology, health, culture, [and] sports…" as well.

The law introduces a number of administrative burdens, including complex review, reporting, and filing procedures, which could present considerable operational costs. Foreign NGOs would no longer be permitted receive foreign funding without being registered in China and would be required to submit their plans and budgets for the year ahead (with any activities not included in the plan strictly prohibited). Moreover, foreign NGOs would have to obtain the approval of designated Chinese sponsors – who may be reluctant to take on such a liability during a period generally characterized by heightened scrutiny.

For security managers, the biggest development may be the transition of oversight from the Ministry of Civil Affairs to public security departments under China's State Council. Not only does the change in responsible agency imply that NGOs and civil society may pose a threat to security, the responsibly authorities now have explicit supervisory, investigative, and enforcement authorities. Foreign NGOs that fail to comply risk having their registration revoked, and their employees risk deported or criminally prosecuted.

NGOs and academic institutions currently operating in China are encouraged to work closely with their in-country partners, affiliates, and host universities to determine what warnings (or assurances) have been provided by Chinese authorities and what impact they believe this pending legislation could have on their future operations. Organizations in these fields may also consult with their private sector peers, particularly those with a more established presence in China, to share best practices for lawfully continuing operations.

**Excerpts from Foreign NGO Management Law**

*SUPERVISION*

Public security organs are responsible for "the annual **inspection of foreign NGOs' representative offices**" and "**conducting supervision** of foreign NGOs and their representative offices' activities, and **investigating unlawful conduct**." (Article 47)

*ENFORCEMENT*

Public security organs may "enter the Foreign NGO's office… to conduct and on-site inspections… **question units and individuals** related to matters being investigated... seal or seize venues, facilities, or property related to the matters being investigated." (49)

*FUNDING*

"Foreign NGOs that have established representative offices **shall use funds from the bank account within mainland China**" (27); "Financial accounting reports **shall be audited by accounting firms in China** and be made public." (29)

*STAFFING*

"Foreign NGOs representative **offices hiring personnel or recruiting volunteers… shall entrust local foreign affairs** service units… **to handle it**." (32)

GROUNDS FOR CANCELLATION / DETENTION

"**Subversion of state power**… Undermining ethnic harmony or engaging in separatism… **Inciting resistance against enforcement of state law** … Gathering state secrets or intelligence… **Spreading rumors**, engaging in defamation… Engaging in or **providing financial assistance for political activities or illegal religious activities**… (59)

# XI. "National security" as a pretext to bolster domestic industry?

While encumbering foreign NGOs may be seen as an attempt to curb negative ideological influence, it does little to address the core issue of a slowing economy. Having achieved decades of sustained growth by investing in manufacturing and infrastructure, Beijing is now looking to transition to consumption and services as key drivers of the economy. With this in mind, it is possible to see how legislation extoled as an effort to maintain national security may alternatively aspire to cultivate domestic *information and communications technology* (ICT) firms.

One of the provisions of the new National Security Law that has garnered significant attention is the "secure and controllable" clause. Although the vague wording of the the law fails to delineate exactly what this may entail, experts believe the provision could require IT companies to transfer proprietary source code to authorities, create *backdoors* in existing platforms for third-party access, and house Chinese *citizens' personal data* on Chinese servers.

Chinese authorities claim this is part of a broader effort to underscore the country's *cyber sovereignty*. Some experts, however, view Beijing's claims that possessing source code or hosting user data on Chinese servers necessarily bolsters its security as a flawed assumption. Instead, they suggest it is a subtle means of exacting concessions from foreign firms and *forcing technology transfer*. Ultimately, this may leave U.S. companies faced with a difficult choice: comply and receive access to Chinese markets on the one hand, or refuse to comply and miss a potentially lucrative opportunity on the other.

One of the looming questions may be the timeline of implementation. For some software and services, current domestic offerings appear to be insufficient alternatives to existing Western technology. Heavy investment in ICT and progress in the innovation of Chinese substitutes, however, could hasten the enforcement of these recently enacted laws and promote national champion firms – all under the pretense of national security.

Private sector security managers are encouraged to become more familiar with the terms associated with ITC and network security (see callout). Additionally, they might better prepare themselves by understanding the penalties for non-compliance, which include fines of up to RMB 500,000 for organizations who violate the laws; closing down of websites; and cancellation of business licenses.

Additionally, as with the Foreign NGO Management Law, firms accused of being in violation of these laws (whether rightfully or not) may be subjected to intensified supervision and inspection. Organizations are encouraged to educate their local and expatriate staff on the possibility of unannounced inspections, referred to often as "dawn raids," and have a plan for providing the information relevant to the investigation without turning over intellectual property or sensitive company information.

**Glossary**

Information and Communications Technology (ICT): the integration of telecommunications, computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

Backdoor: a feature or defect of a computer system that allows surreptitious unauthorized access to data.

Citizens personal data: a citizen's name, birthdate, identification card number, personal biometric data, profession, residence, and telephone number recorded electronically or by other means.

Cyber sovereignty: An increasingly common phrase used by Chinese authorities suggest the right to govern network administration in accordance with national security needs.

Forced technology transfer: a process by which technology, knowledge, skills and manufacturing methodologies are transferred from one country or company to another.