
CHINA
RISING

China Rising

Modern historians have long argued that an essential segment in the study of human evolution is inextricably tied to the basic understanding that societies generally emerge, progress and fall cyclically. Such frequency in social evolution is not just a consequence of endogenous factors, it also results from the impact of the external environment, be it close - neighboring constituencies vying for the same resources - or far - as part of a larger, global economy.

History teaches us another fundamental truth, predominantly unveiled in social sciences: humans are inherently prone to believing in the danger of the unknown, the fear that uncertainty - when present in life - brings an intolerable level of complexity in handling daily activities. Economists, in tandem with the larger group of social scientists, ascribe the word "risk" to this angst.

Risk lies in everyday life. From birth to death and in between the terrestrial episode called life, humans experience a sophisticated relationship with risk and utilize it as a powerful catalyst to furthering their interests. We fear the unknown not just in temporal terms - e.g.: what will tomorrow be? - but also in more practical, present-day terms, that is, what will happen today?

In assessing the rectitude of our daily decisions, the analysis of the environment we live in becomes of critical importance. There emerges then the need to know, understand and act on a variety of variables that make up our ecosystemic reality. Neighbors are a major part of that reality.

The indubitable observation that humans are 'sociable animals' implies a life in community, which in turns posits the sharing of interests, destinies and geography. We share our lives with neighbors, other humans whom we don't fundamentally know and whom we believe are different from us. Neighbors, in continental philosophy, are the 'constitutive other' as opposed to 'same'. Neighbors are different, and because of that, they must be hazardous to our very existence, hence "hell is other people" (Jean-Paul Sartre).

Consequently, our desire to know the 'other' and what they're undertaking forces us to constantly be in a question mode: ergo, we resort to spying. Espionage is ingrained in basic human instincts from cradle to grave. First, we ape our relatives, then our acquaintances and later our neighbors. In that quest for knowledge, humans recklessly spy on each other in a bid for power. Once they determine with a reasonable degree of comfort the neighbor's strengths, the overwhelming tendency is to match it, surpass it, annihilate it, keep it at a politically acceptable level, or use a combination of all these options if the socio-historical continuum of events demands it.

Doubtless, the need to control the military and economic standing of neighbors is the quintessential, albeit hidden, dogma of modern geopolitics. Doctrinal differences may abound, but a studious analysis of contemporary events demonstrates clearly that wars and other man-engineered crises have historically proven to be good ways to rebalance powers among neighbors, or more precisely, within geographical zones. Crises, facts have shown, drive innovation and quality of life.

Espionage is not a recent discipline within political science. It has been a staple of human history for the past 2,000 years and even before. Throughout history, nations have risen or fallen based on their ability to collect data from rivals and use that body of knowledge to gain a competitive edge. History also suggests that societies that show a disinclination for 'outer research' of their environment, and consequently, a significantly lower number of exogenous interactions - be it cordial or belligerent - with others have been weakened over time. The high frequency of wars between nations in the 'Old Continent' explains the relative superiority that Europe had over, say, Amerindians and Africans for the past few centuries, first in slavery and then colonization.

Espionage is rooted in modern life:

After two atrocious global wars, countless medium-size conflicts and a dogmatic cold-war between capitalism and communism, political and military leaders seem to have finally gauged the idiocy of

lethal conflicts with planetary implications. The notion of 'détente', that is, the easing of strained relations in the political phraseology, gives nations the imaginary assurance that they may all coexist pacifically and a major conflict is preventable once greater cooperation between societies subdues the inherent quest for power that causes hostilities.

Acquiescing that there exists a permanent détente within the current geopolitical landscape is an optical illusion because it goes counter the very human urge to monitor the neighbor in order to know him or dominate him, if not annihilate him. This can be very easily illustrated in instances where spies are caught in so-called 'friendly' territories. Take the example of Israel's Mossad agents being arrested in the United States.

The nuts and bolts of modern state espionage lie in a sophisticated and complex apparatus that all nations, and peculiarly global superpowers, have invented to carry out data-collecting and monitoring activities in peace time. Embassies, with their massive bureaucracies, specialized technocrats and their diplomatic inviolability, are preeminent on that list. They are essential in monitoring the host country's social dynamics and report to their respective governments. Simply put, an embassy is, de jure, a stranger turned neighbor.

Next are supranational organizations that populate the global political, social and economic sphere. Their local representations and periodically published studies may also serve an intelligence purpose. Finally, aid agencies and so-called 'humanitarian' organizations are critical in gauging so-called 'underdeveloped' nations' economic ability and progress in their development. It is no coincidence that major countries in the developed sphere do not customarily accept 'aid programs' from their counterparts unless excruciating circumstances dictate that such refusal would be politically unacceptable.

Strategic studies and the modern economic literature are replete with topics referring to Japan's, and to a lesser extent, Asian dragons' ability to use economic espionage at the end of the Second World War to gain a competitive edge over erstwhile powers such as the United States and Great Britain. The necessity to monitor and direct the continent's economic reconstruction, and the

panic of a potential dominance by communist Russia, also led the United States to implement the Marshall Plan in Europe from 1948 through 1952.

Businesses thrive from spying more than the military:

A noteworthy myth in today's world is that espionage is principally the province of military strategists and national armies. Evidence from authoritative business intelligence magazines, leading governmental studies and a massive body of knowledge from academia have clearly explained the causal relationship between firm profitability and espionage. Differently stated, governments tend to always transfer intelligence data to their domestic industries, whether they are at war or at peace.

As a result, the military-industrial complex benefits considerably from intelligence and such prerogatives are then disseminated into other firms in the economic fabric. As an illustration, it would be fairly understandable that a firm like Boeing, which derives a substantial portion of its revenues from government's contracts and sale of military aircrafts, is more attuned to certain developments in US intelligence gathering than a financial services giant like Citibank.

Nevertheless, businesses have also parlayed their gargantuan economic clout into a very successful data-collection enterprise. The plethora of tools available to business executives nowadays is strikingly sophisticated and effective. Even if it is not exhaustive, a good analysis of such tools must look at their source and their degree of macro-economic interconnectedness.

On one hand, external mechanisms allow at the macro-level business enterprises to gather information from competitors and control how such information can be utilized to thwart rivals, increase their own market primacy, or do both. When they share a community of interests vis-à-vis a new market or are in an oligopolistic situation, companies are routinely willing to join hands provided, of course, that the risk-payoff ratio of a single venture is not immensely superior to that of a joint venture. Tacit collusion, that is, the market situation where two firms agree to play a

certain strategy without explicitly saying so, is a fine illustration of business intelligence sharing.

In practice, firms engage in economic espionage via economic sections of embassies, chambers of commerce, lobbying groups, industry groups, specific studies from consultants, and monies granted for academic research in particular fields of interest. Concomitantly, they guard against intelligence threats by massively supporting intellectual property laws.

On the other hand, a sophisticated internal approach allows companies to stay abreast of latest developments within their industry. First and foremost, they hire to their corporate boards or for senior positions, experienced former government officials and high-rank military leaders who had been privy to high-value strategic insights during their public tenure.

This is immensely beneficial to the hiring side because a former cabinet member, a congressman or a four-star general, can possess a breadth and depth of experience and knowledge of past, present and future topics that is considerably worth more than countless external consulting reports. Second, economic intelligence departments and government relations departments also fulfill data gathering roles through research, lobbying and interacting with industry groups.

Cyber-warfare, the new cold war:

As the planet becomes technologically more intertwined, novel tools and modus operandi are being made available to governments and private interests to collect specific intelligence. These tools and procedures are an intricate combination of old and new procedures which simultaneously penetrate nations' military, economic and social constructs to extirpate valuable bits of knowledge.

Defense experts are calling these emerging asymmetric conflict tools 'cyber-warfare'. Due to the plethoric ramifications they present and the simultaneous dual tasks they may serve to fulfill

(attack and defend) when engineered in certain ways, I label this group Modern Cyber-warfare Gear ("MOCYG").

MOCYG, as it stands, involves the offensive use of various techniques to derail a nation's infrastructure, perturb the military and financial systems of a country with the aim of crippling its defense responsiveness and the integrity of economic data, or accomplish other destructive aims based on the attacker's incentives and strategy. Security specialists and military researchers have classified these techniques into 5 major groups: computer forensics, viral internet tactics, assault on computer networks or software, hacking and espionage.

The idiosyncratic power of cyber-crime lies in its 'stateless' nature, its capacity to be inexpensively controlled and deployed, and the vast damage it can exert. Given the judicial vacuum created by cyber-warfare techniques, nations are rushing to build up legislative safeguards to prosecute offenders even though criminologists argue such undertakings are largely inefficient at the moment.

A memorable cyber-criminal event occurred in Estonia in 2007 when more than 1 million computers, allegedly from Russian-based servers, were used to simultaneously cripple state, business and media websites in a modus operandi analogous to the "shock and awe" military tactic. That attack ended up costing Tallinn's authorities tens of millions of US dollars.

China, a cyber-giant in progress:

Upward socioeconomic trends in the People's Republic of China are well known to international masses and covered profusely in western news media. So are Chinese authorities' singular understanding of democracy and human rights as well their overt wish to play a bigger geopolitical role in world affairs. However, the quiet revolution China is experiencing lies within the astronomical investment country authorities are making in top notch universities so as to catapult China into the top league of technological giants, along with the United States and Japan. Given

the size of such educational outlays, Chinese authorities must believe that a major competitive edge can be gained in the technology field and such advantage can be converted or transferred into other sectors of their mushrooming economy.

Top western sinologists and other think tanks are closely monitoring these academic developments because they understand the basic notion that future geopolitical dynamics will inextricably be tied to how successful Chinese will be at leveraging technology to boost their future 'global penetration'.

The smart tactic is that, while future chief engineers are being trained at world-class institutions such as University of Science and Technology at Hefei, Harbin Institute of Technology, Beijing University and Tsinghua University, China is concurrently putting a veil of secrecy around its information systems and cyber-infrastructure. The country may be notorious today for its copyright infringement cases or intellectual property violations, but it is inconspicuously gearing up for tomorrow's technological primacy that its expansionist aspirations may dictate.

China also investigates currently available ways and means to unearth state-of-the art synergy tools that can be leveraged between its major government departments and state agencies as it prepares to enter the 'knowledge economy'. Authorities view this coordination effort as an indispensable step forward because it adds another layer of centralization to a government structure that is built around the canon of 'consolidated power'.

More specifically, country leadership has summoned top minds in technology and auxiliary fields to synergistically engineer the future cyber-infrastructure that will solidly mark China's imprint in the digital landscape. This task is colossal, and the vastness of it effects precludes obviously an analytical granularity. Several hundreds of thousands of Chinese computer engineers, regrouped under ad hoc commissions, think tanks and strategy centers are the backbone of this emerging 'digital army'.

They work under the aegis of brilliant specialists whose unquestioned patriotism and in-depth expertise are unparalleled at such high seniority levels; this group includes Liang Guanglie, Wan Gang and Li Yizhong. The first is the current minister of defense, who works in conjunction with the People's Liberation Army and the Central Military Commission to manage the largest military force in the world (ca. 3 million) and oversee its strategic evolvement.

The second is the head of the Ministry of Science Technology and is mechanical engineer and auto expert. The third is the Minister of Industry and Information Technology, a cabinet position pivotal for the country's information systems development.

Anemic US IT investments:

Equipped with this super cyber-security gear, China seems to be winning, or is in a significant position within, the ongoing global cyber-war. In a sense, the country is not an 'emerging' superpower as western analysts and social science specialists would like to call it. It is already a superpower in the fullest sense of the concept.

The term 'emerging superpower' is presently preferred in academic and business literature as well as in media parlance because it is more politically palatable to the elite and other classes of citizens in traditionally influential economies (G8) who fear the psychological and social implications of welcoming new colossi in the select club of the powerful.

Security experts and top military minds in the United States are truly concerned that the Chinese massive IT investment dwarfs America's and do not hesitate to point to the geopolitical implications of such a chasm. They note that the countless cyber-attacks from China and Russia are just a start of the new cyber 'Cold War' of the 21st century.

It is a fact that many foreign-engineered digital attacks have targeted many industrialized

countries' military systems, power grids, and financial infrastructure in the past few years. Yet governments and military forces at present have limited capacity to detect or infiltrate the attacker, counter the attack, and prevent future assaults.

US defense officials and business leaders understand the looming threat but believe its intensity and gravity constitute a hyperbole. However, authoritative statistics from the Government Accountability Office, US Congress reports, and academic studies indicate evidently that the world leader has not shown hitherto the political willpower to tackle the digital gap in its cyber-security infrastructure.

Truth be told, politicians in Washington, Pentagon strategists, and the intelligence community at large have long known of and understood the nature of the menace. Notwithstanding, a series of geopolitical events forced them to transfer certain topics into budgetary oblivion at the credit of more pressing, more 'visible' national security threats that are effortlessly noticed by constituents (e.g.: terrorist attacks).

A few factors explain Washington's inability, or budgetary lethargy, in addressing the cyber-warfare threat. First is the geostrategic complacency derived from the fall of communist Soviet Union and the ensuing inertia that global unipolarism usually creates.

Second, America's military apparatus is currently 'distracted' by two ongoing wars and engaged in a host of relatively minor security missions around the world. Adding to those involvements, there is the corollary 'war on terror' that has mobilized since 2001 colossal resources to thwart further domestic attacks.

'Domestic' in this sense refers to an incredibly enormous geographical area because it encompasses US conventional soil and the related territories, American overseas diplomatic missions, its military bases, transnational organizations where the US holds significant strategic interests (e.g.: NATO headquarters and military stations), and the countless aid, religious, and

humanitarian outposts around the world.

Third, the diversity and criticality of issues at hand force the US government and congressional leaders to prioritize their budgetary efforts. The current economic despondency bodes ill for any serious endeavor in tackling underinvestment issues in information technology because the country is pecuniarily limited and cannot afford to continuously print money (risk of inflation and currency devaluation) or borrow from... China.

US budding cyber-security grid is solid:

Despite the socio-economic gloom, the Obama administration has shown in the past 6 months a strong level of commitment in assuring the integrity of the nation's information assets. He appointed late December Howard Schmidt, a renowned computer security specialist and former Microsoft security executive, as White House cyber-security czar. Other high-profile nominations have followed in the army ranks and other key departments and government agencies such as Homeland Security, Treasury, the FBI and the CIA.

The efforts appear to be coordinated and effectively reaching their desired goals, from the Pentagon's launching of a giant "cyber-command" unit to the CIA's and FBI's massive 'hiring spree' of computer engineers and cyber-security specialists. International cooperation with other allies is also part of the undertaking; US intelligence agencies are thus partnering with foreign counterparts such as Britain' MI5 and MI6, Israel's Mossad, Germany's Bundesnachrichtendienst (Federal Intelligence Service, BND) and Militärischer Abschirmdienst (Military Counterintelligence Agency, MAD) to address emerging threats.

Private interests are equally gearing up. Businesses are investing massively in IT infrastructure and upgrading computer networks, and working jointly with government agencies. They are also granting rising subsidies to think tanks and academia to help in this effort.

The combination of efforts has to be successful because an absence of effectiveness in cyber-warfare measures can be 'lethal' to US global supremacy. Judging by the great havoc cyber attacks had catapulted onto Estonia in 2007, hyperbola ought not to be barred in this topic.

Based on the latest estimations, US nominal GDP is nearly 3 times that of China ($14.5 trillion vs. $4.5 trillion), but the latter's healthier growth rate is helping bridge that gap gradually. Thus, many forecasters - and the proverbial 'conventional wisdom' - assume that it will take Beijing many decades to attain America's economic clout and level.

That said, in the hypothetical scenario that a cyber-warfare erupts between both countries, a stronger China may only need to considerably crush US economic productivity and therefore its GDP to claim victory and financially surpass its rival. Absent effective security systems, China, or any other foe, may only need to assault vital arteries of the US military-industrial complex: power grids, financial transaction systems, Federal Reserve System, US Armed Forces' computer systems and networks, Congress' and White House's IT infrastructures, etc. It's easy to imagine the massive damage electricity failure can do to a country's transportation, financial, and military systems.