Thoughts on a Competitive Strategy with China

LCDR Robert "Jake" Bebber USN

Disclaimer: The views expressed here do not represent those of the Department of Defense, Department of the Navy, or the U.S. government.

- A winning competitive strategy will slow China's economic growth, or even cause it to begin to contract. A slowing/contracting China will be forced to shift resources *toward internal controls* and *away from power projection*, make China less attractive for foreign direct investment, inhibit Chinese civil-military fusion/innovation, and create doubt in the information control regime the CCP has instituted to remain in power.
    - Civil-military fusion is a national strategy to maximize linkages between the military and civilian sector to build China's economic and military strength simultaneously. Xi Jinping personally oversees the Central Commission for the Development of Military-Civil Fusion. The CCP's aim is to essentially fuse the defense and commercial economies. CCP economic policies and resource distributions have a goal of achieving military innovation and growth.
    - Therefore, any strategy pursued by the U.S. & its friends, partners, and Allies, which does not inhibit China's economic growth or cause its economy to contract is unlikely to prevent a CCP-dominated China from achieving global supremacy.
- China has acute vulnerabilities that can be exploited via cyberspace operations. These include, but are not limited to:
    - Dependence on Western technology, access to global markets, foreign direct investment, foreign manufacturing, importing of energy resources, food supply, information assurance and security of the information control regime, security of critical infrastructure, fragile financial markets
    - It is reasonable to assume that the PRC is attempting to address information security vulnerabilities associated with the above points. However, the overriding need to maintain a pervasive surveillance and information control systems is fundamentally at odds with erecting an impenetrable information security regime (as policy makers in the U.S. know all too well). Therefore, this will remain an enduring vulnerability.
    - **An important vulnerability/liability of the Chinese system is its acute paranoia and hyper-nationalism**. Information-based campaigns can have great effects among a population prone to this thinking. The system is designed to assume that threats – internal and external – abound. *Use this to our advantage!*
- The size of the PRC economy, its global dependencies, and the growth of a PRC-created information environment globally create a massive attack surface from which to pursue this strategy. From a U.S. perspective, this creates far more opportunities to generate large-scale enduring strategic effects **now**, rather than investing considerable resources into exquisite, fragile capabilities designed solely for military effects – **effects which are likely irrelevant to China's overall strategy of global dominance.**
- Off the top of my head, here are some lines of effort organized around a **cyber-enabled geoeconomic/geoinformational strategy to slow/contract China's economic growth**. Many other supporting operations can be done in conjunction with these Lines of Effort that do not

directly involve cyberspace operations (such as enacting trade regulations, public diplomacy, military exercises). Under each LOE, I am highlighting how cyberspace operations can support or enable. This should not be considered all-inclusive by any means. In fact, these LOE's and their supporting cyberspace operations all complement one another and are interrelated, thereby creating larger systemic perturbations.

- **LOE1: Undercut the Belt & Road Initiative** – make China less reliable/desirable as an economic partner
  - LOO1: Penetrate and exploit information networks of Chinese State-Owned Enterprises (SOE's) – SOE's are the main participants in the BRI and should not be considered "off limits" as a strategic target because SOE's are the linchpins of China's policy to use economics to promote state interests, and the fusion of state interests with corporate interests. Being postured to penetrate and exploit SOE networks, the U.S. might:
    - Create operational inefficiencies
    - Slow the tempo and speed of decision-making
    - Re-direct resources into "losing ventures", creating more "sunk costs" that must be backed up by the state
    - Reduce the quality of products and services
    - Exacerbate bureaucratic rivalries within the organization
    - Create fissures and distrust between the SOE and the CCP security services
  - LOO2: Penetrate and exploit Chinese financial institutions which serve as the principal financers of BRI initiatives. The U.S. might:
    - Conceal potential default risks for individual projects, thereby encouraging more investment in projects which are failing or high-risk
    - Create distrust in the financial system by making it appear that banks "favor" some SOE's over others, thereby "propping up" SOE's that are more inefficient
  - LOO3: Elevate target nation "antibodies" to Chinese investment. The U.S. might:
    - Conduct clandestine or non-attribution social media campaigns highlighting political corruption (most BRI agreements come because of Chinese bribes/cooption of local politicians, business leaders, etc.), "imperialism with Chinese characteristics," human rights violations, environmental devastation, religious persecution, etc.
    - Promote alternative investment options, such as Indian or Japanese investment projects
- **LOE2: Degrade R&D associated with "Made in China 2025"** – impede, retard, disrupt, misdirect efforts by China to achieve self-sufficiency to increase dependence on Western technology. There are 159 Chinese universities and research institutes affiliated with the PLA, state security services, or the government in some way. **The networks at these institutions are notoriously insecure**.
  - LOO1: Garbage in, garbage out – use China's cyber exploitation and intellectual property and technology transfer programs to input "bad" data into the system,

driving PRC RDTE down dead-ends or away from areas that disadvantage the U.S./Allies

- LOO2: Penetrate and exploit hardware associated with research networks to sub-optimize research results
- LOO3: Exploit patronage networks, personal rivalries, and cultural need to "save face" by disrupting patronage networks, exposing (or creating the appearance of) corruption, promoting the work of inferior researchers/scientists while undercutting the influence of superior researchers/scientists

- **LOE3: Attack principal drivers of Chinese economic growth** (large scale capital investment financed domestically or via foreign investment) and productivity (efficiency) – U.S./Allied cyberspace operations might:
  - LOO1: Penetrate and exploit regional and local government networks (far more insecure than national level networks) to:
    - Promote corruption by targeting local political leaders and administrators
    - Conceal investment risks, or create them where none exist
    - Disrupt timing and tempo of financing
    - Divert investments from some regional projects to others to create friction between provinces and the national Party
  - LOO2: Suboptimize supporting infrastructure associated with development. For example, associated transportation networks supporting large scale capital investment in a region might be exploited to create sustained inefficiencies (in other words, the "trains don't run on time"). This would also have the effect of reducing productivity efficiency. **Create "lost work hours" in the system**.
  - LOO3: Target individual, high profile Chinese investors to create friction between them, the CCP and global corporations (Can also support LOE4 – "Big Fish")
  - LOO4: "The Google Effect" - Conduct influence campaigns within global corporate shareholders and employees to create internal friction and opposition to doing business in China or jointly with Chinese companies (Also supports LOE2)
  - LOO5: Penetrate and exploit United Front networks – illuminate UF penetration and influence over foreign corporations, institutions; steer UF attempts to penetrate institutions that support U.S. deception and denial plans
  - LOO6: Leverage growing understanding of neuroscience to develop and deploy capabilities in the information space which nudge Chinese population behavior into areas that inhibit productivity, create social frictions, exacerbate unfavorable demographic trends, and further drive government resource allocation away from areas of competition with the U.S.
- **LOE4: Create fissures between the Chinese people and CCP** – force CCP to reallocate more resources toward maintaining domestic control. U.S./Allied cyberspace operations might:

- LOO1: "Lying Eyes" – Most Chinese surveillance camera systems are easily penetrable and lack security. Exploit these systems to make them "see what we want them to see"
- LOO2: Manipulate Social Credit system – make the loyal appear disloyal, and vice versa. This can support LOE1, LOE2, and LOE3
- LOO3: Penetrate and exploit local CCP cadre networks and institutions (i.e., soft targets not affiliated with security or noteworthy Party organs) to create friction with national CCP
- LOO4: Exploit online gaming networks and companies ("Strike of Kings", "League of Legends", "DotA") – Tencent and Netease are two of the largest gaming companies in China, and both have a global presence. This can also support LOE5
- LOO5: Produce online content, create "influencer" personas – most internet users in China watch online videos via smartphones (males tend to prefer gaming, females tend to prefer videos on daily life) – this content can slowly "nudge" behavior in directions that support U.S./Allied objectives. This can also support LOE5.
- LOO6: "Big Fish" – the recent experience of Jack Ma (Alibaba) suggests the CCP has deep concerns over those who might become a threat to Xi Jinping. Exploit networks associated with others to exacerbate fears within the CCP of alternative power centers developing, questioning loyalty.
    - A parallel effort might highlight corruption and wealth disparities in online social platforms that suggest the CCP is not concerned about the poor or middle class
- LOO7: "Blowback Mountain" – using information capabilities, manipulate surveillance, monitoring, and behavioral systems against the Chinese people by exploiting fissures between consumers, Chinese companies, security services, and the Party apparatus. Accelerate the process of Chinese "netizens" finding and exposing information the system is designed to keep hidden.

- **LOE5: Increase global "antibodies" toward use of Chinese information technology, telecommunications infrastructure** – generate mass advocacy among foreign audiences against PRC telecommunications through clandestine or non-attributable means
    - LOO1: Make Huawei, China Telecom, ZTE the next Global NSA/CIA – The National Security Agency / Central Intelligence Agency has a global reputation. Conduct clandestine or non-attributed influence campaigns that begin to link Chinese telecommunications to "China NSA"
    - LOO2: Penetrate and exploit Chinese telecommunication network operations to reduce consumer reliability (especially if it can later appear to be in support of Chinese monitoring activities) – example: throttle bandwidth, re-route network traffic through China, make random communications "cut in" and appear to be monitored (imagine random people around the world reporting that in the middle of their conversation they believe they "hear" Chinese security agencies talking about them)

        - LOO3: Reduce the quality and reliability of Chinese telecommunications products (hardware and software)
        - LOO4: Penetrate and exploit networks of foreign major suppliers to Chinese telecommunication networks
    - **LOE6: Reduce quality of critical imports** of integrated circuits, mineral products, vehicles, metallurgical products, chemicals, rubber, primary plastics, and other raw materials
        - LOO1: Penetrate and exploit Chinese SOE's associated with resource extraction, refinement, and distribution (Sinopec, China National Petroleum Corporation, etc.)
        - LOO2: Penetrate and exploit infrastructure and utilities – slowly increase inefficiency and suboptimize performance over time (this can also support LOE4)
        - LOO3: Penetrate and exploit major suppliers to China of critical imports, to include subcontractors and "supplier to suppliers" networks
        - LOO4: Penetrate and exploit networks of Chinese universities and institutions conducting RDTE that improves capabilities of Chinese resource extraction and refinement
        - LOO5: Supply chain interdiction/manipulation/exploitation
        - LOO6: Conduct influence campaigns on foreign populations to illuminate environmental destruction by China (coral reef destruction, overfishing, air pollution, etc.)
        - LOO7: Conduct influence campaigns **within China** on environmental destruction and against technologies that we may not want China to leverage (e.g., create China's own "anti-nuclear power" movement)
        - LOO8: Penetrate and exploit maritime port networks in China and those operated by Chinese companies – reduce the efficiency of maritime connectivity using the Liner Shipping Connectivity Index
- To execute these lines of effort, we will require a comprehensive set of **metrics by which to evaluate the campaign**
    - There are generally accepted measures of economic performance, but they often do not tell the entire story. Gross National Product, Gross Domestic Product, government spending, worker productivity is commonly used, but given the opacity of the Chinese system, are unlikely to be reliable.
    - It might be better to de-emphasize GDP and GDP per capita (given the CCP's use of these for propaganda purposes and lack of transparency) and instead consider other indicators such as:
        - Personal income
        - Aggregate debt
        - Factory productivity
        - Unemployment
        - Trade
        - Foreign reserves
        - Financial sector health

    - There are many industry-specific tools to evaluate the campaign. For example, the Liner Shipping Connectivity Index scores countries and container ports based on level of integration into established liner shipping routes. The Kearney Global Cities Index evaluates an urban area's performance in five areas: business activities, human capital, information exchange, cultural experience, and political engagement. The China Global Investment Tracker is a comprehensive data set covering China's global investments and construction (usually associated with BRI). The Fortune Global 500 and Brand Finance Global 500 provide insights into the economic "clout" of Chinese companies.
    - There are specific, strategically directed, programs, that are worthy of tracking. These include utilization of digital payment platforms (Alibaba's Alipay and Tencent's WeChat Pay) as well as the introduction of the digital renminbi (DCEP – digital currency electronic payment).
    - Specific to trade and resource as China's exports of Rare Earths, which are central to many high technology industries. Vulnerability to coercion due to reliance on Chinese exports has caused countries like Japan to significantly reduce rare earth imports from China from 90% to 58% in a decade.
    - Other industries to evaluate might be: global presence of Chinese telecommunications, infrastructure, surveillance, "Smart Cities," port operations, undersea cables, airports and airport operations, land transportation networks (road and rail). Related industries include pharmaceuticals, health care, food supply/security, environmental factors, manufacturing,
    - Some indexes and concepts to evaluate include: economic complexity, innovation, foundational research, the Global Competitiveness Index, the Global Innovation Index, Global Health Security Index, the valuation of the Science and Technology Innovation Board on the Shanghai Stock Exchange (the "Star Market"), gross domestic spending on R&D, space-launch capabilities (active satellites by countries of ownership, ratio of payloads to launches, success of key rocket series, number of manned spaceflights, R&D spending on spacecraft manufacturing, launch costs per system, space station capabilities), Internet penetration (to include Global Speedtest Index, broadband download speeds, 5G coverage, Internet usage by device, e-commerce activity, Digital Silk Road growth vs. other providers, "Freedom of the Net" – level of internet and digital freedom)
- Related to the above points, the U.S. requires a Strategic Latency & Disruption Evaluation and Assessment capability:
    - Identify areas of emerging disruptions, financial investments, dual use, radical leveling and emerging technologies
    - Pay particular attention to emerging disruptions associated with neurosciences (ability to access, assess, and affect the brain – both on an individual level and on mass populations)
    - Ability to monitor and evaluate sources of U.S. and Allied power, identify areas of potential comparative advantage for investment – areas where the U.S. might introduce disruptive technologies
- The U.S. requires a Cognitive Warfighting entity that possess the following capabilities:

    - ISR of the cognitive domain space – monitor the health of the decision-making process as it extends into alliances, domestic institutions, foreign institutions, elites, and general populations
    - Preparation and execution of cognitive/counter-cognitive campaign plans
    - Evaluate, exercise, inform and harden U.S. decision processes (federal, state, local); evaluate and exploit foreign decision processes
    - Conduct and coordinate influence campaigns, both friendly and hostile
    - Develop, monitor, and evaluate friendly foreign decision-making processes
- Integrate and build upon evaluation and analysis capabilities such as Harvard University's Thresher (monitoring social media in China), Repari Analysis (fin/tech). SquirrelWerks (cyber threat intelligence), Defense Group Inc, SOSi, etc.

Concerns and Objections

The principal objection to any strategy that seeks to inhibit the rate of China's economic growth, or even contract its growth, rests on certain assumptions:

1. What hurts China, hurts the U.S. (and the rest of the world)

2. Attacking China's economy attacks its people

3. Invites retaliation or escalation

4. May push the CCP to be more aggressive

5. The Department of Defense does not "do" economic war

What hurts China, hurts the U.S. (and the rest of the world)

Major industries, trade associations, and Chinese propaganda have raised alarms at the prospect that recent trade policies and larger efforts to "decouple" from China pose an equal or greater risk at hurting the U.S. In the short term, and in certain sectors which still depend upon Chinese dominated supply-chains, this is probably true, though the actual harm to individual Americans is a matter for debate. What is often ignored is that the CCP has adopted several policies promoting self-sufficiency ("Made in China 2025") across a spectrum of industries and services. China long ago began the process of decoupling from foreign industries. That process will continue, irrespective of U.S. or global desires.

Such an objection also presupposes that additional American investment in capital projects will not offset the effects of reduced Chinese economic growth. Major domestic initiatives in American shipbuilding, roads, semiconductors and information technology, renewable energy development, energy production, steel, minerals, pharmaceuticals, health care, and other investments would not only further insulate the U.S. from Chinese economic coercion but would also promote substantial economic growth that permits the U.S. to maintain its economic edge over China.

In fact, China's economic growth is the principle means by which it can finance its ambition to achieve global hegemony, to include supplanting the liberal international order with a techno-authoritarian order where the CCP makes the global rules. The drive for military-civil fusion will only

enhance the military capabilities of the PLA forces, which will ultimately be used to coerce the United States and the rest of the world. China's military growth is tied to its economic growth, and dependent upon it. **The only way to effectively reduce China's military capabilities will be to reduce its economic performance.**

Attacking China's economy attacks its people

The past several decades has seen a significant percentage of the Chinese people being lifted out of poverty. The most important driver of improved living standards in China was the global investment in China, principally led by the United States. As foreign investment is reduced, this will place the burden of domestic programs more on the ruling Chinese Communist Party. Indeed, the CCP now enjoys a "guns AND butter" approach toward economic development because its economy is still be propped up by foreign investment. This strategy seeks to force the CCP into harder choices as its economy is slowed further, or ideally even contracts. However, that choice rests with the CCP, not with the United States. If they decide to invest less in its people and more in the military, that is not the fault of us.

Invites retaliation or escalation

Frankly, the long-standing policy of "restraint" did nothing to discourage malicious Chinese behavior, Chinese state-sponsored cyber-enabled economic warfare, cyber-attacks, or intellectual property theft and conversion. The Chinese have only stepped up these and other efforts in its bid for global supremacy and control of the global information ecosystem. In many ways, whether the U.S. conducts this strategy or not, the CCP still sees it in its best interests to continue its pursuit of global power.

Adopting an economic-oriented strategy does have the advantage of opening additional avenues of coercion for the U.S. and Allied powers that fall short of kinetic operations. The choice to retaliate or escalate places more dilemmas on the CCP leadership, as it requires diversions of shrinking resources.

This strategy may push the CCP to be more aggressive

The CCP's stated goals and its timetable for achieving them are already under pressure as its window of opportunity is closing. The CCP has taken a more aggressive approach because of the nature of its leadership, specifically Xi Jinping. It will remain aggressive if he or others like him remain in power, not because anything the U.S. does or does not do. It is a fallacy to think that the U.S. can "drive" CCP strategic ends until there is a change in who is running the CCP, or there is a change in Xi Jinping's sense of what he can accomplish. The CCP is going to be more aggressive *regardless* of what the U.S. does.

The Department of Defense does not "do" economic war

First, this flies in the face of historical precedent of U.S. military operations (and the employment of military forces historically) in support of blockades, interdictions, strategic bombing, privateering and commerce raiding. U.S. and Allied forces operate in peace time in support of international sanctions regimes to this day. The rejoinder is that there is no formal declaration of war that would justify military operations in support of an economic strategy. While it is true that most of Western thought provides a clear delineation between "war" and "peace," this is new and unique in history. Russian and Chinese cyberspace forces (as well as other nations) have been conducting operations in support of their larger economic and political objectives for the past two decades, and the U.S. is slowly coming around toward understanding that persistent engagement in the information space is a reality of the larger great power competition space. From a practical perspective, only DoD possess the large enough force design and resources to effectively conduct economic campaigns. Other agencies, even those with covert action authorities, do not possess the scale necessary and are better suited to complimentary, targeted operations.

Final Thoughts

No one is really going to like any of this. There are significant antibodies within the U.S. national security system against this type of thinking. While there is emerging, bipartisan consensus that the U.S. is in a form of global or strategic competition with China, there is no articulated end state or theory of victory, other than perpetual competition. This proposal is an attempt to drive at an end state, using principally non-kinetic, cyber-enabled information campaigns to achieve a strategic end state.

While many who review this document will have resistance, it is also certainly true that executing this program will cost much less than recapitalizing the U.S. military, modernizing our nuclear forces, or any other of the long laundry lists of wishes in DoD programs. It can have disproportionate strategic effects compared to the investment required. This should not be taken to mean that the U.S. should execute this program *instead of* modernizing its nuclear forces, recapitalizing its Navy, or continuing to invest in military capabilities.

If some entity or agency, inside or outside the DoD, wants to take this project on (or something like it), and wants to discuss these or other ideas, I am standing by to assist in any way.