WARNING ORDER

China Prepares for Conflict – and Why We Must Do the Same

Fred Fleitz, Editor
Gordon G. Chang
Dean Cheng
Kevin D. Freeman
Frank J. Gaffney, Jr.
Bill Gertz
Admiral James "Ace" Lyons, Jr.
Dr. Peter Navarro
Lindsey Neas
Senator Jim Talent

Center for Security Policy Press

ISBN-13: 978-1533302199
ISBN-10: 1533302197

Warning Order: China Prepares for Conflict, And Why We Must Do the Same
is published in the United States by the Center for Security Policy Press,
a division of the Center for Security Policy.

June 1, 2016

THE CENTER FOR SECURITY POLICY
1901 Pennsylvania Avenue, Suite 201 Washington, DC 20006
Phone: (202) 835-9077 | Email: info@securefreedom.org
For more information, please see securefreedom.org

Book design by Adam Savit
Cover design by J.P. Zarruk

CONTENTS

CONTENTS **3**

EXECUTIVE SUMMARY **5**

(U) WARNING ORDER: REQUIRED PREPARATIONS FOR CONFLICT WITH CHINA **9**

FOREWORD **11**
Frank J. Gaffney, Jr.

INTRODUCTION: CROUCHING TIGER - CHINA ACTS, AMERICA DITHERS **13**
Dr. Peter Navarro

CHINA 2016: GEOSTRATEGIC AND MILITARY CHALLENGES **25**
Senator Jim Talent and Lindsey Neas

A TURBULENT CHINA SHAKES THE WORLD **39**
Gordon G. Chang

CHINA, UNRESTRICTED WARFARE, AND THE CHALLENGE TO AMERICA **55**
Kevin D. Freeman

COUNTERING CHINA'S OBJECTIVES IN THE WESTERN PACIFIC **81**
Admiral James "Ace" Lyons, Jr., USN (ret)

CHINESE MILITARY BUILDUP **87**
Bill Gertz

ESPIONAGE AND CYBER: CHINA STEPS UP A COVERT WAR **95**
Fred Fleitz

PROSPECTS FOR EXTENDED DETERRENCE IN SPACE AND CYBER: THE CASE OF THE PRC **113**
Dean Cheng

ABOUT THE AUTHORS **127**

EXECUTIVE SUMMARY

This book presents the case for a "Warning Order" to be issued immediately to America's armed forces and their command authorities. Its purpose would be to authorize the preparations needed to contend with the rapidly emerging prospect of conflict with Communist China.

The essays in Warning Order have been written by some of the most prominent and respected experts and security policy practitioners of our time. They warn that the Obama administration has dithered over the unraveling of the U.S. position in the Middle East and – notwithstanding a putative "pivot" to Asia – largely ignored that strategic region, as well. China has been emboldened to challenge and, if possible, to displace the once-dominant role played by the United States, both in the Western Pacific and globally. The upshot is a growing peril to America, her allies and interests, both in traditional battlespaces and in new domains, like outer space and cyberspace.

Highlights of the contributors' essays include the following:

- Former U.S. Senator Jim Talent discusses the scope of the military threat from China and how it has been exacerbated by huge cuts to the U.S. military by the Obama administration.
- Chartered Financial Analyst Kevin Freeman explains how China is engaged in "unrestricted warfare" and preparing for "total war" with a view to defeating America around the world and in every battlespace. Freeman notes how, as a result, we now face threat vectors that involve not only the conventional, nuclear and cyber arenas. The PRC is also putting itself in a position to wage economic warfare, for example, through crashing the U.S. stock exchange, intellectual property theft and currency warfare.
- Author and columnist Gordon Chang assesses how problems with China's economy and domestic power struggles are likely to lead to the remilitarization of Chinese politics and a surge in Chinese belligerence abroad.
- Journalist Bill Gertz discusses the huge growth in China's military, especially its missile arsenal and navy. Gertz says Chinese anti-satellite weapons and MIRVed missiles pose special threats to U.S. security and

endanger the ability of the U.S military to prevail in the event of military conflict with China.

- Heritage Foundation scholar Dean Cheng discusses a related issue: how China's notions of extended deterrence in outer space and cyber space is not only a policy of deterrence, but one of coercion, designed to compel its opponents to carry out actions that advance Chinese objectives.
- Former Commander-in-Chief of the Pacific Fleet Admiral James "Ace" Lyons and University of California Professor Peter Navarro present complementary analyses of how Chinese expansionism in the South and East China Seas is threatening U.S. and regional security, as well as economic interests. Like Kevin Freeman, Adm. Lyons and Dr. Navarro note the growing threat posed by the Chinese navy, its doctrine to destroy U.S. aircraft carriers and how China's naval capabilities threaten to neutralize the historic advantages of the American navy, in part thanks to cuts in military spending by the Obama administration.
- Career intelligence professional Fred Fleitz discusses the growing dangers posed by actual and prospective Chinese cyber attacks and espionage, including how it has tried to recruit American students who visit China to spy for Beijing. Fleitz warns that U.S. officials have done little to counter these ominous developments.

The growing threats from China discussed by this book's authors require significant responses by the United States. Some responses are needed immediately. These include:

1. Recognizing the growing threat from China and its preparations to engage in total war against the United States. America's leaders must educate themselves and the public on the implications of this reality and the necessity of acting now to contend with it.
2. Immediately forming a new bipartisan congressional commission – like the influential 1998-1999 Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China (the Cox Committee) – to assess growing threats from China and recommend policies to address the associated perils for our military, America's economy, cyber assets and intelligence community. This commission's report should feature recommendations on, among other things, steps the United States must take to defend against Chinese efforts to collapse the U.S. stock market and Chinese currency manipulation.
3. Reversing the devastating effects of sequestration on the U.S. defense budget by restoring Pentagon spending to at least 2008 levels. America's

land, naval, air, missile, nuclear, space and cyber forces must be enlarged and modernized to counter China's growing military and other global threats.

4. Discarding the Obama administration's "benign neglect" strategy in the Asia-Pacific region and implementing a robust strategy to: protect U.S. strategic interests; enforce commitments to our allies; and stand up to China. This must involve, at a minimum: routine naval operations in the South and East China Seas to defend freedom of navigation and our other vital interests there; increased deployments of land, air and missile assets in the region, including missile defense systems in Japan and North Korea and returning U.S. naval forces to Subic Bay, Philippines; and a publicly reiterated pledge by the President to protect the security and sovereignty of Taiwan, South Korea and Japan.

5. Adopting a new approach in dealing with Chinese officials that involves defending unapologetically American interests and equities and calling out China when it engages in belligerent, threatening and unfriendly behavior. America must stop showing weakness by looking the other way when China commits such actions. American officials must no longer be silent when Chinese officials deride or ridicule the United States during diplomatic meetings or otherwise abuse military-to-military exchanges or exercises.

6. Announcing and enforcing a new policy of zero-tolerance toward China's growing cyber warfare and intelligence efforts against the United States and making it clear that, when China engages in such actions, there will be consequences that will include trade sanctions, deporting Chinese officials and businessmen from the United States and, if necessary, retaliatory U.S. intelligence and/or cyber countermeasures.

It is impossible at the moment to say with certainty whether Communist China will actually exercise the option for engaging in conflict against the United States and/or its allies. What we can say, though, is that America can no longer afford to ignore the fact that the Chinese are acquiring that option – and may take our continued indifference to that possibility as an invitation to engage in aggression against us or our friends and interests, regionally or beyond. That must not be allowed to happen.

(U) WARNING ORDER: REQUIRED PREPARATIONS FOR CONFLICT WITH CHINA

DRAFT
UNCLASSIFIED*

Washington, D.C.
05031020Z16

1. (U) Situation. The People's Republic of China (PRC) is incrementally, but relentlessly, putting into place in its own region (notably, the East and South China Seas) and elsewhere around the world the capabilities required to engage decisively in military conflict with the United States and its allies.

(U) China's preparations include:

- The acquisition and deployment – both at home and increasingly in global choke points – of advanced air, sea, land and space systems and asymmetric capabilities that appear designed to: 1) interdict allied forces, 2) deny them access to and the ability to operate in strategically important areas and 3) otherwise achieve the destruction and defeat of the U.S. and/or its allies;
- The fielding of sufficient numbers of modern aircraft, ships, missiles, space weapons and nuclear forces to secure for China quantitative and, in some areas, qualitative superiority, at least regionally;
- People's Liberation Army cyber warfare operations that are intensifying in sophistication, aggressiveness and effectiveness against both official and private sector targets;
- A variety of means of challenging and undermining the United States' economic security, including by threatening: the dollar's reserve currency status, Wall Street and other financial operations, and U.S. access to and relations with key trading partners;

- High-intensity intelligence, information and influence operations against the United States and its allies; and
- Amassing the dedicated military and dual-use industrial capabilities necessary rapidly and substantially to expand, and/or recover from battle-damage to, the PRC's current conventional and nuclear arsenals.

(U) It is not possible at this time to ascertain Chinese intentions or whether, if they do seek to precipitate a conflict, when and where it might begin. Our posture must not be based on assessments of such intentions, however, but be rooted in a clear-eyed, capabilities-driven threat analysis.

2. (U) Tasking**.** All DOD agencies, military services and combatant commands are hereby ordered to take such steps as are required to achieve at the earliest possible moment levels of readiness and power-projection needed to deter and, if necessary, to defeat any Chinese aggression. U.S. capabilities required to perform such missions over the longer term are to be identified and acquired at the earliest possible time. Wherever practical, useful and consistent with operational security considerations, the support and assistance of allied militaries should be obtained for this purpose.

Secretary of Defense

UNCLASSIFIED

FOREWORD

Ever since Richard Nixon opened relations with Communist China, Chinese intentions have been a matter of incessant and often fevered speculation in this country. In particular, national security and regional experts, non-governmental organizations and office-holders alike have endlessly debated whether the People's Republic of China could be brought into a U.S.-dominated international order and world economy in a manner consistent with American interests and, better yet, as a partner in opposition to mutual adversaries (e.g., the Soviet Union, North Korea and the global jihad movement).

The contents of this book suggest that this controversy is pretty much settled. Under successive regimes – and most especially that of the incumbent Chinese ruler, Xi Jinping – the Chinese have relentlessly and unmistakably striven to put themselves in a position to challenge, and ultimately to displace, the post-World War II Pax Americana with a new order. It would return China to what they considered to be its rightful place as the Middle Kingdom, the preeminent global power strategically and economically.

The distinguished contributors to this book may still have somewhat different views about China's motivation or intentions. They may also arrive at different conclusions about the magnitude of the impediments to the realization of such ambitious, and ominous, Chinese goals.

But our authors have documented from their various perspectives and fields of expertise a reality that can no longer be safely ignored: The PRC is putting itself in a position to engage in conflict with the United States across a broad front and potentially with decisively devastating results.

The purpose of this collection of essays is not to say that Beijing has decided actually to take such a step. That may or may not be the case.

Given, however, the actions we can see that China has taken to date – including preparations for economic warfare; dominating and denying us the use of strategic chokepoints; employing an immense, military and dual-capable industrial base to produce vast quantities of ships, planes and other military hardware; achieving

the capacity to engage in disruptive space operations, preemptive thermonuclear strikes against the U.S. homeland and infrastructure, cyberwarfare and information, influence and espionage operations in this country – it is foolhardy, and irresponsible, any longer to construe this conduct as non-threatening.

Our hope is that this Warning Order – a technique long used by the U.S. military to put its units on notice of an impending danger that requires countervailing action – will move our nation past a now-irrelevant debate about Chinese intentions and onto a footing rooted in a focus on capabilities, one that enables us to deter the PRC's future use of existing, and anticipated, threats to our security and vital interests.

Frank J. Gaffney, Jr.
President and CEO
Center for Security Policy
25 April 2016

INTRODUCTION: CROUCHING TIGER - CHINA ACTS, AMERICA DITHERS

By Peter Navarro

Will there be war with China? That may well be determined by which presidential candidate wins the White House this year, and what policies the new administration adopts.

The threat of conflict is real. Cambridge University's Stefan Halper does not wish to "alarm people," but he soberly notes the "profound differences" that China is "prepared to settle by force." Harvard's Graham Allison likewise warns of a "Thucydides Trap," in which a rising China plays the upstart Athens to America's Sparta, and fear leads to an arms race and war. Michael Green of the Center for Strategic and International Studies hedges this bet: "The US has to contemplate a future with China that will probably be benign but could very well be difficult, intense, and, in the extreme scenario, hostile."

If a rapidly militarizing China seeks only to protect its homeland and the global trade routes it needs to prosper, the world can probably relax. But if China is also committed to expansionism and seeks to push the US military out of the Asia-Pacific region and take territory and resources from its neighbors, there may be conflict on the horizon.

Beijing's sense that a rapid military buildup is necessary to defend its homeland is rooted in China's "Century of Humiliation." From the 1830s until the end of World War II, foreigners, from the British, the Russians, and the Japanese to the Germans, the French, and the Americans, committed brutal acts—rapes, beheadings, port seizures, land grabs. To Toshi Yoshihara of the US Naval War College, "the historical lesson the Chinese have learned is 'never again.' Never will China be weak because this is what invited foreign aggression."

That China's military buildup is necessary to defend its trade routes is likewise historically based. Even as Deng Xiaoping began China's remarkable transformation in the 1970s from a socialist, autarkic, and continental power into the global trading force it is today, his naval commander, Admiral Liu Huaqing, began to

build the modern navy Deng's new mercantilist China would need. In this sense, Liu was what Yoshihara and his coauthor James Holmes from the US Naval War College have called a "Mahanian" figure, an allusion to Alfred Thayer Mahan, the 19th-century American military theorist who pioneered the concept of global naval force projection as critical to economic prosperity.

Liu first articulated the three-step Mahanian strategy China appears to be following today. In step one, China breaks the bonds of the First Island Chain, which runs from the Kuril Islands and Japan through the center point of Taiwan and across the Luzon Strait to the Philippines and down to Malaysian Borneo. As Dean Cheng of the Heritage Foundation notes: "If the First Island Chain is in the hands of countries antagonistic towards China from Beijing's perspective, then it is a barrier to China's ability to reach the open ocean."

In step two, China breaks through the Second Island Chain, which runs from the Kuril Islands to New Guinea, directly through the anchor of American power in Asia, the island fortress of Guam.

Finally, by 2050, China becomes a global blue-water navy projecting its power around the world.

If China does indeed succeed in controlling the waters of the Asia-Pacific, it will only do so through the defeat—or acquiescence—of the United States. Of course, any such outcome would open the door to aggressive and revisionist Chinese behavior toward its neighbors, in much the same way a revanchist Russia now bullies Eastern Europe.

Much is at stake strategically and economically in this new "great game." Strategically, whoever controls the South China Sea's gateway to the Indian Ocean, through the narrow and perilous Malacca Strait, also controls Southeast Asia—and perhaps East Asia, too, given that much of the oil that lights the lamps of Japan and South Korea must first pass through the South China Sea.

In addition, the modern "silk and spice" trade accounts for a third of global shipping, while the waters of the East and South China Seas are also home to fertile fishing. Meanwhile, beneath more than a million square miles of seabeds may lay petroleum reserves comparable to the Persian Gulf's.

In the South China Sea, China has already "salami sliced" the Paracel Islands from Vietnam and flaunts floating oil rigs flanked by flotillas of Chinese warships in waters claimed by Hanoi. China has similarly taken Macclesfield Bank and Scarborough Shoal from the Philippines and remains locked in a long-term battle over Second Thomas Shoal. China even eyes the rich gas fields of Indonesia's Natuna Islands—almost 1,000 miles from the Chinese mainland.

In the East China Sea, Japanese military forces likewise remain locked in an upward-spiraling dispute over the Senkakus, five small rocky islands with a landmass of less than two square miles. This bitter confrontation, tinged by ultra-nationalism, has already led to mass anti-Japanese riots on the Chinese mainland, as well as moves toward an increased war-fighting capacity on the part of Tokyo, and threatens to draw US forces into the conflict.

Many observers seem befuddled by China's increasing aggressiveness over such small "rocks in the sea." However, the 1982 UN Law of the Sea Treaty entitles nations commanding any such habitable rocks to a full 200-mile "exclusive economic zone" that conveys natural resource rights to the holder. Thus, as the Cambridge scholar Stefan Halper explains, a continental power like China can greatly extend its maritime rights in "concentric circles" with a "leapfrog effect" simply by taking control of small, disputed islands.

The Law of the Sea Treaty has also greatly complicated US-China relations. China takes the novel position—nothing in the treaty supports it—that freedom of navigation and overflight by military vessels and aircraft are restricted not just within a nation's 12-mile territorial limit but also within the 200-mile zone. If China's "closed seas" doctrine were accepted, this would give China control over the most lucrative trade routes in the world.

This jurisdictional clash has already led to numerous confrontations, from China taking hostage the crew of a downed US reconnaissance plane in 2001 to a more recent provocative barrel roll by a Chinese fighter jet over a Navy patrol aircraft. On the high seas, Chinese forces have similarly buzzed the unarmed USS *Impeccable*, an ocean surveillance ship, and attempted to block the USS *Cowpens*, a guided-missile cruiser, from operating in international waters.

One key reason nuclear bombs never fell during the Cold War is that the US and Soviet Union talked. For example, the American president and Soviet premier shared a "hotline" starting in 1963, and naval commanders regularly engaged in "bridge to bridge" communications.

No such "circuit breakers" exist today between China and the United States. Former Assistant Secretary of Defense Kurt Campbell frames the strategic divide this way: "The United States is all about showing what we've got. Look how powerful we are." China, by contrast, "seeks deterrence often through uncertainty, leaving potential adversaries with questions as to just how capable they are." David Lampton of Johns Hopkins University adds: "So we have us believing clarity leads to deterrence and China thinking that obscurity and non-transparency will."

There is a similar strategic divide when Chinese and US military ships find themselves in close proximity—as they are increasingly wont to do. From the American perspective, bridge-to-bridge communication is critical to prevent miscalculations. To China, Stephanie Kleine-Ahlbrandt of the US Institute of Peace explains, such communications are "seatbelts for the speeders."

Indeed, Chinese military commanders believe it is good for their American counterparts to worry about what a Chinese response might be since this will make them more cautious. They sometimes seem oblivious to the fact that, as Campbell says, "things can get out of hand."

The twin pillars of Chinese military strategy—area denial and asymmetric warfare—likewise point to possible conflict ahead.

Mark Stokes of the Strategic Studies Institute translates anti-access and area-denial practices as "interdiction." China's goal, according to Bonnie Glaser of the Center for Strategic and International Studies, is to "prevent other countries, particularly the United States, from having the capability to intervene in waters or airspace near China in a crisis."

China's companion asymmetric warfare strategy is "not seeking to counter the United States military on a one-on-one basis, as occurred during the Cold War between the US and the Soviet Union," according to Bill Gertz of the *Washington Free Beacon*. Instead, "the Chinese are developing niche weapons systems." Toshi

Yoshihara, the War College scholar, says: "Part of the dark beauty of China's anti-access/area-denial strategy is that it relies on really very striking cost asymmetries. For example, an aircraft carrier costs billions of dollars while a salvo of Chinese missiles is priced in the millions; and it may take only one Chinese missile getting through to score a mission kill. It's not a competition the US can win. The Chinese can build many more missiles than the Americans can build capital ships."

Ashley Tellis of the Carnegie Endowment for International Peace describes China's heavy reliance on tip-of-the-spear missiles to attack targets in all dimensions as "the poster child of asymmetric warfare." As he explains, "The key thing ballistic missiles and land-attack missiles bring to the table is suppressing air defenses. Once you suppress air defenses, then you can bring in conventional fighter bombers." "So if you're in Taiwan, or you're in Japan, or even if you're in Vietnam," says Dan Blumenthal of the American Enterprise Institute, "you face the prospect of Chinese missiles that can hit you. So every time you're negotiating with the Chinese, you have a gun to your head."

It's not just China's neighbors who are at risk. Lyle Goldstein of the US Naval War College sees China's new highly maneuverable, hypersonic airborne glide vehicle as particularly threatening to US forward bases and aircraft carriers because of the "immense speed that it re-enters the atmosphere." Gertz elaborates: "All of our missile defense capabilities are designed for ballistic missiles and other targets that have a fairly predictable trajectory. Once you have a maneuvering warhead that's traveling at up to ten times the speed of sound, it has made our missile defenses relatively ineffective."

China's inventory of sea mines—the largest in the world—and its burgeoning submarine fleet fit hand-in-glove with these strategies. The purpose of mine warfare is not to sink ships per se but rather deny access through a combination of psychological terror and the lengthy time required to effectively sweep mines. (During the Gulf War, for example, despite expensive US minesweeping efforts, two Iraqi mines costing less than $50,000 each scored a mission kill on a billion-dollar cruiser, the USS *Princeton*.) Bernard Cole of the National Defense University views sea mines as a particularly difficult hurdle in any Taiwan scenario because Taiwan has

only two major ports. Says Yoshihara: "If the Chinese can conduct the first move, and sew mines in the approaches to those ports, Taiwan would essentially be sealed off. There are no other alternative ports that would be able to provide the sufficient throughput [i.e., free travel] to keep Taiwan going."

China's mines work synchronously with China's diesel-electric submarines. Virtually all of China's new subs (by 2020, according to Pentagon estimates, Beijing will have amassed the world's largest fleet, at some 69–78 boats) are equipped with foreign air-independent propulsion systems—and many of its old subs are being retrofitted. Notes Richard Fisher of the International Assessment and Strategy Center: "Conventional diesel-electric submarines are already very quiet and difficult to find. With air-independent propulsion, they become phenomenally more deadly, especially to American aircraft carrier battlegroups."

Yoshihara envisions a nightmare scenario of forward-deployed Chinese conventional submarines lying in wait for an American carrier strike group and then launching their long-range, anti-ship cruise missiles in "salvo fires" to overwhelm fleet defenses. Such a scenario not only recalls Joseph Stalin's adage that "quantity has a quality of its own," but also calls into question the widely held belief that the technological superiority of the American military machine will always triumph.

Princeton's Aaron Friedberg offers this sobering perspective: "The American intelligence community has been surprised by the quality of the systems the Chinese have been able to field, and part of the reason is that they've been stealing intellectual property." As a result, China can now produce drones identical to their American counterparts. It has also begun to field the most advanced fighters, like the Chengdu J-20, decades before the Pentagon expected; and, unlike budget-constrained America, which cancelled its own advanced fighter, the F-22, China will churn out massive numbers of whatever weapons systems it chooses in much the same way America once did during World War II to overwhelm the often technologically superior German forces.

China has also openly embraced a two-pronged "carrier killer" strategy to deny US forces free access to the Asia-Pacific while moving into disputed islands in

the East and South China Seas, into the hills of North Korea, and even into the Indian state of Arunachal Pradesh, which China claims as "Southern Tibet."

How will the peace be kept under these mounting pressures? America has certainly made a big bet on the power of economic engagement to transform China from a belligerent, authoritarian regime into a peace-loving liberal democracy. However, as Ian Fletcher of the Coalition for a Prosperous America notes: "Economic growth in China has not led to its becoming more democratic. It has simply led to a more sophisticated, better-financed form of authoritarianism."

What is needed is a more textured understanding of the role of economic interdependence in deterring—or creating—conflict. If a country like China is heavily dependent on trade for goods vital to national security, that country may actually be more likely to go to war as economic interdependence rises. Such interdependence helped lead Germany—fearful that both France and Great Britain would deny the food, iron ore, and oil it needed to prosper—to attack in 1914. Nor was this simply German paranoia: France and Britain both openly discussed embargoes leading up to the war, in much the same way analysts like T. X. Hammes of the National Defense University today recommend the "economic strangulation" of China in the event of a conflict.

The Princeton scholar Aaron Friedberg's cautionary note about trade may be worth recalling here: "Countries that have intense trading relationships do not necessarily have good strategic or political relationships; and, historically, countries with intense trading relationships have sometimes gone to war with one another."

As for the nuclear deterrence argument, Carnegie's Ashley Tellis counters that China's emergence as a credible nuclear power actually increases the risk of conventional war "because China has steadily acquired the capabilities to prevent the United States from coming to the assistance of its friends in Asia."

Toshi Yoshihara explains the stability-instability paradox underlying such risk: "If the Chinese can superimpose their anti-access strategy, that might create strategic space for China to conduct conventional offensive military operations within the Asian maritime theater. And so, having nuclear weapons does not necessarily

ensure that there will be no war. It simply opens up different avenues for different kinds of wars."

If we cannot count on economic engagement, trade interdependencies, or nuclear weapons to deter conflict with China, what other pathways to peace remain? Some will no doubt say that instead of pivoting to Asia, the US should stay at home and leave the region to the Chinese. But as *Forbes* columnist Gordon Chang has pointed out: "America's first line of defense is not Alaska and California but rather South Korea and Japan," and America's forward bases play an important strategic role in missile detection and defense. It is also useful to remember here that America is, and ever has been, a trading nation; and a freely accessible Asia offers the most rapidly growing markets in the world.

Barring a neo-isolationist retreat, what must our policy be? Any answer must begin with the observation that if America merely seeks to match China bullet for bullet, the result will likely be an escalating arms race that either bankrupts one or both countries or ends with a very big bang.

Michael Pillsbury, a Pentagon analyst, offers a sobering warning: "If we face a thousand Chinese anti-ship missiles, there's no way to stop them all. The world we're moving toward is a world in which the Chinese economy has surpassed us and is growing toward being twice as powerful as us. That means if they want to, their defense spending can be focused on us; and it can exceed our defense spending."

How can our next president deal with this growing Chinese encirclement? The answer lies in what the Chinese themselves call "comprehensive national power," a concept deeply rooted in Sun Tzu's famous maxim that "to subdue the enemy without fighting is the acme of skill." As Wu Chunqiu of China's Academy of Military Science puts it: "Victory without war does not mean that there is no war at all. The wars one must fight are political wars, economic wars, science and technology wars, diplomatic wars. Although military power is an important factor, in peacetime it usually acts as a backup force."

Consider, for example, the national synergies required just to build a nation's "backup" military capabilities. Such synergies begin with a strong economy, capable of both manufacturing weapons and generating tax revenues to pay for them. However,

to have a strong economy, a nation must have a highly skilled work force—and therefore an equally strong education system.

At the same time, rapid innovation and technological change can only take place in the presence of a financial system delivering the capital investment to drive research and development, and a tax system rewarding entrepreneurship. Nor will any domestic economy prosper without ready access to foreign markets. Such access not only requires strong alliances among trading partners. It also demands freedom of navigation, which brings the synergistic process right back to the need for a strong military to keep the seas and skies open for trade.

David Lampton, the Johns Hopkins scholar, says that when American power is healthy in this comprehensive way, the Chinese will respect the US. If America declines, however, "the Chinese are going to be more difficult to deal with."

Still, a nation with a strong economy, a fine education system, a stable political order, a wealth of natural resources, and a superb labor force that is poorly armed will still be easy prey for any well-armed adversary with malicious intentions. Patrick Cronin of the Center for a New American Security describes the kind of "balanced force for the 21st century" America needs "in large enough numbers" to achieve peace through military strength: "I need my carriers, aircraft, and submarines. I need stealth, and I need to be able to patrol the sea lines. At the same time, I need to keep investing in cyber and space technologies and unmanned aerial vehicles and long-range unmanned systems because those technologies could be game-changers."

Aaron Friedberg of Princeton believes it is equally critical to reduce the vulnerability of American forward bases in Asia through a four-corners strategy of hardening, dispersing, diversification, and force restructuring.

"Hardening" means moving fuel supplies and weapons caches deep underground, siloing aircraft, and pouring literally tons of concrete on literally tons more of steel rebar to fortify runways and buildings, barracks and piers.

"Dispersing" means redeploying both bases and ships in ways that "would make targeting a much more complicated issue for the Chinese." Toshi Yoshihara recommends, for example, dotting Japan's Ryukyu Islands with an archipelago of

much smaller facilities rather than just offering big bull's-eyes like Okinawa and Guam.

"Diversifying" means expanding American bases and facilities into countries not currently hosting a large American presence, like the Philippines and Vietnam. Says Dan Blumenthal: "If Chinese decision makers have to think about hitting many targets in many countries, that is a far bigger deterrent than just having to hit a few bases in Japan or a US aircraft carrier."

Friedberg also wants to turn the asymmetric warfare and area-denial tables right back on China through force restructuring. Here, James Holmes recommends moving away from those sitting-duck carrier strike groups beloved by the Navy's top brass to an array of Virginia-class attack subs deployed across the major chokepoints of the First and Second Island Chains.

As for other weapons systems, one of the biggest questions facing the next president is likely to be the need for a new long-range strategic bomber. A $21.4 billion development contract was awarded to Northrop Grumman last October, but questions remain as to how many might eventually be built—and who ascends to the White House in 2017 will certainly matter. As Michael Auslin of the American Enterprise Institute has stated in making the pro-bomber case:

> "Our youngest B-52 bomber is fifty years old and we've had close to three generations of pilots flying the same planes—grandfathers, fathers, and sons. They are wonderful airplanes, but they can't survive against today's automated missile defense systems. Plus, we only have twenty B-2 Stealth Bombers, and they're getting old as well. So we need a new bomber, and we need the F-35 in far greater numbers to be able to clear the ground and the skies if need be, and we need to do this as much for military reasons as for political reasons; and it'll actually bring more stability to Asia, not less."

Beyond these concrete steps, Georgetown lecturer Phillip Karber calls for a policy of "reciprocal response" vis-à-vis China: "You go into arms control and you reduce your forces, then we reduce our forces. You start doing provocative things like adding more and more missiles and threatening our bases and our allies, we will respond."

Ironically, even though such threats make this a good time to build up alliances, false promises and neglected relationships have squandered the opportunity.

Consider the Obama administration's failed "pivot" to Asia, announced with fanfare in 2011. The Pentagon is supposed to increase the percentage of its total naval fleet in the Pacific to 60 percent by 2020. However, because that fleet continues to shrink, the US will actually have fewer ships in total numbers in Asia in 2020 than when the pivot began in 2011. "As diplomatic and deterrent signals go," says James Holmes, "this makes the pivot a pretty bush-league thing."

Pat Mulloy, a former member of the US-China Economic and Security Review Commission, takes criticism of the White House's military-centric pivot one step further, claiming the pivot strategy reveals a more fundamental lack of understanding about America's pressing need to rebuild comprehensive national power. Advises Mulloy: "Now the president says we have to pivot toward Asia because we have a rising China. But China is rising because we're running massive trade imbalances. So wouldn't it make more sense to simply rebalance our trade deficit and not continue to have American consumers feed China's rise? That would be the truly smart way to pivot towards Asia."

To peacefully counter the serious economic and security challenges posed by a rapidly rising China, there must first be political consensus. However, achieving any such consensus will be difficult in an open democracy where: economic interests are divided by their stakes in the China trade; lobbying groups would rather fight each other than band together in common cause; an authoritarian Chinese government is able to exert significant media control over the China narrative; and both Western journalists and American universities engage in systematic self-censorship.

In truth, this "house divided" assessment goes a long way toward explaining why democracies in the West, and America in particular, have been so slow to respond to a revanchist China. If this head-in-the-sand perspective persists, however, the story can only end badly.

CHINA 2016: GEOSTRATEGIC AND MILITARY CHALLENGES

By Senator Jim Talent and Lindsay Neas

Edited from remarks by former Senator Jim Talent (R-MO) at the Center for Security Policy Capitol Hill National Security Group Lunch

February 11, 2016

A lot of what I do now is related to China. I don't consider myself a China scholar, in the same sense as someone who reads Mandarin. But I have served on the U.S.-China Economic and Security Review Commission for over three years, and I keep up on the news regarding China. I see it is as my job to translate what various China experts are saying about developments there into a lexicon that my former colleagues, and the broader public, can understand, and to explain why what China is doing matters to the United States.

It's a pleasure to be with you today to discuss those developments.

If we want to figure out what is going on with China's leaders and what the United States ought to do in response, we must first ask what China is trying to achieve in East Asia, and why, and what America should be trying to achieve in that region, and why. You can't decide how you're going to get someplace until you know where you want to go. You can't shape the actions of others until you know where they are trying to go and what is motivating them to try to get there.

It's important in doing this not to see China's words and actions through American eyes. Our leaders have the tendency to assume that deep down China's leaders and people are really like we are, that they want the same things we want. This tendency is sometimes referred to as "mirror imaging." That's a tremendously patronizing thing to do to any foreign country but especially the Chinese, who are of course an ancient people with a long history that has its claims upon the present, and who are currently led by the Chinese Communist Party (CCP) – a group of men with definite goals, strong will, burning ambitions, and consistent purpose. If America's leaders don't understand that, they're not going to understand where China's

objectives conflict with those of the United States and what America needs to do to deter them and either reconcile that conflict or succeed in a competition with them.

So let's look first at what the Chinese have been doing. Nearly every year since 1989, China has been increasing its military spending by double digits; this has translated into a major, almost unprecedented buildup of their military strength – a buildup which in the last five years has been bearing fruit. I won't discuss the buildup comprehensively; the China Commission does that in its annual Reports, and I highly recommend the chapter on military modernization in the Commission's 2014 Report.[1]

Here, briefly, are some features of the program:

China has created a large and modern navy, which, at the present rate will, by 2020, be substantially larger than America's. Its vessels are highly capable and armed with long-range, advanced, anti-ship missiles and air-defense missiles.

China is upgrading its nuclear arsenal and is on track to more than double the number of nuclear warheads capable of striking the U.S. homeland over the next few years.

They already have the world's largest and most lethal inventory of conventional ballistic missiles as well as large numbers of highly capable and long-range ground, air and sea-based cruise missiles. They will continue to expand, diversify, and improve their missile inventory, enhancing their ability to coerce or use force against the United States and its allies and partners in Asia. China now is able to threaten U.S. bases and operating areas throughout the region, including those that it previously could not reach with conventional weapons, such as Anderson Air Force Base on Guam.

They have almost 2,000 capable fighter aircraft and are on track to introduce two new fifth-generation fighters, which they will likely add to their inventory between 2017 and 2019. China also appears to be developing a new long-range stealth bomber.

---

[1] *2014 Annual Report to Congress*, U.S.-China Economic and Security Review Commission, November 20, 2014, http://www.uscc.gov/Annual_Reports/2014-annual-report-congress, 282-346.

China is significantly upgrading its intelligence, surveillance, and reconnaissance systems and improving amphibious capabilities.

According to the Defense Science Board, China already has offensive cyber capabilities that can inflict existential damage – damage comparable to that caused by a nuclear exchange – on America's critical infrastructure and upon our society.

It's important to understand the enormous logistical advantage China has in any prospective conflict or confrontation in the East and South China Sea. America's forces are spread all over the world; it takes two to two and a half weeks, for example, to steam from the West Coast of the United States to the East and South China Seas. China's military forces are already in its near seas; in the event of a confrontation, they will be able to assemble their power in a matter of days, and since presumably they'll be the ones starting the confrontation, they will have the lead time to prepare and America won't.

It's clear from China's literature that its leaders understand the next major conflict will be an information war and that domination of the information sphere will be tremendously important. They understand that the Achilles heel of deployed American forces is our reliance on satellite communications. That makes their development of comprehensive anti-satellite capabilities particularly relevant, and ominous. Again, the best and most recent survey of China's capabilities in this regard was produced by the China Commission, in its 2015 Report.[2]

The best way to think of the Chinese buildup is this: they are constructing a missile-centric military to take advantage of an asymmetric vulnerability of the United States. That's the result of a lesson they learned almost 20 years ago.

In 1995-96, the Chinese engaged in sabre rattling over political developments in Taiwan. China's rulers feared that Taiwan might declare its independence. In response, President Clinton sent two aircraft carrier task forces through the Taiwan Strait. The Chinese could do nothing in response to this show of force. It was very humiliating for the CCP, but their strategists studied and learned from that encounter. In particular, they determined that much of the striking power

[2] *2015 Annual Report to Congress*, U.S.-China Economic and Security Review Commission, November 17, 2015, http://www.uscc.gov/Annual_Reports/2015-annual-report-congress, 272-337.

of the United States Navy is concentrated in its aircraft carriers and the cruise missiles aboard our destroyers and cruisers.

Let's suppose such an episode were to occur today. If a President today sent a carrier task force into the Taiwan Strait during a period of heightened tensions, the carrier would face the very real prospect of scores of Chinese missiles coming from all different directions and from nearly every platform – submarines, fighter aircraft, bombers, and surface combatant vessels of all sizes – in the Peoples Liberation Army Navy (PLAN). Some would be cruise missiles travelling near the ocean's surface; some would be ballistic missiles, meaning that they would first enter the exosphere and then upon reentry would come screaming down at the carrier, or other major surface combatant, at supersonic speeds. In other words, China can threaten our carriers, which now cost over $13 billion per ship, with a salvo of missiles that costs them a couple of hundred million dollars. That is an asymmetric vulnerability.

China's leaders may well believe an American president would not risk losing a carrier under those circumstances. And if they believe that, it may well encourage them to begin a confrontation in the first place.

In fact, China is already triggering confrontations; the shift in the balance of power – the growing ability of China to exploit America's asymmetric vulnerability – is already affecting China's calculations in the East and South China Seas.

China claims sovereignty over virtually the entirety of those seas and the island formations in them. In the South China Sea, for example, their claims, illustrated by their infamous "nine-dash" line, encompasses Taiwan, and extend virtually to the shores of the Philippines, Malaysia, Vietnam and Brunei, and also include waters legitimately claimed by Indonesia. This is not some small matter. The South China Sea is twice the size of Alaska. Some of the most important shipping lanes pass through these waters. Petroleum reserves beneath these waters may equal half of Saudi Arabia's proven reserves.

To enforce these claims, China unilaterally exercises the rights of a sovereign, presenting its neighbors with the choice of either acceding de facto to its claims or starting a shooting war with a regionally dominant military power that has a large, modern navy and a tremendous missile arsenal looming in the background.

Four years ago, Chinese forces blocked off the Scarborough Shoal and took control of it from the Philippines. They are trying to do the same thing to the Second Thomas Shoal. Two years ago, China stationed an oil rig in waters also claimed by Vietnam and began constructing man-made islands upon reefs and islets. Those concrete islands are now military installations. For years, the Chinese have been flooding the Senkaku Islands, which Japan administers, with overflights, fishing boats and coast-guard vessels.

China has declared an "Air Defense Identification Zone" over much of the East China Sea; it may soon do the same in the South China Sea. Chinese maps claim Taiwan and much of their near seas as Chinese territory; they refuse arbitration or resort to international law over their claims.

In short, China is acting like an aggressive hegemon in its near seas. There is nothing subtle whatsoever about what they are doing, and no sign that they will stop unless and until they are confronted with costs that outweigh the perceived benefits.

It's a purposeful, tailored strategy designed to exploit the shifting balance of power in the Western Pacific. It was originally referred to as a "coercive but non-kinetic" set of tactics – but of course the underlying threat is that the confrontations will only remain non-kinetic if China's neighbors do not resist.

So far it's been a winning strategy. To be sure, China has not achieved everything it wanted, but it has achieved a lot; and while the CCP has suffered reputationally – in the sense that other countries in the region are more suspicious of China than they were five years ago – that has not yet resulted in coordinated action sufficiently effective to stop China's momentum.

One of the advantages of this for China so far is that it has been a no-lose proposition. The worst that happens to them is they don't gain ground. They may get everything they want. They may get part of what they want. But they don't lose any ground.

Why is China doing this? What interests are they seeking to advance? There are three:

The first is economic and strategic. China wants unfettered access to the resources in its near seas and control over its strategic environment.

Another is nationalistic and historical. China has historically been the "middle kingdom" in Asia. That's how they view themselves. And what does that mean? It means that Chinese leaders believe that the countries along their periphery should be in various stages of vassalage to China.

It's important to understand the broader implications of this view. A Japanese scholar once said to me that "whereas we [the democratic countries] view the world horizontally, China views the world vertically – with China at the top of the food chain. In such a world, there is no equality; there is no rule of law.

Since World War II, the United States and its allies have created an international system that fosters, however imperfectly, a) free and equal access to the seas, air, space, and cyberspace, b) neutral rules governing trade, and c) the resolution of disputes according to accepted norms, where smaller countries are at no disadvantage. It's sometimes referred to as a "norm-based international system." China's leaders have accepted the benefits of such a system to facilitate their ascent, but resist complying with the restrictions; they see the world as one where "the big dogs get the benefits" within their respective spheres of influence, and they view Asia, or East Asia at least, as their sphere.

When Xi Jinping talks about a "new great power" relationship with the United States, he's referring to this conflict in visions of the world; he wants an Asia, including the Pacific Rim, dominated by China's influence rather than by neutral rules which, more or less, treat all nations equally.

Finally and probably most importantly, is the determination of the Chinese Communist Party to retain unquestioned political power. The CCP understands that to retain control they need not just the repressive organs of the state but some degree of legitimacy among the people. They have made clear beyond doubt that they do not intend to seek that legitimacy by creating democratic institutions or by tolerating differing points of view. Instead, they have made a kind of implicit deal with the Chinese people; in return for continuing the CCP regime without democratic elections, the Party will create a better quality of life, will reverse what it calls "the century and a half of humiliation" from roughly 1800-1950, and will restore China to its rightful place as the dominant power in Asia.

Make no mistake: that is a very powerful factor in motivating Chinese policy in the Western Pacific. Nothing is more important to the CCP than retaining its unchallenged hold over Chinese society. In a way, it's a classic expression of the authoritarian impulse to direct dissent outwards; the CCP distracts the people from the repression of the State by focusing them on alleged grievances against their neighbors and the United States.

Those are the three interests China is seeking to advance with its policy in the East and South China Seas. Again, it is important to understand that the CCP views those interests as vital, which means they are not going to abandon them, or the policy by which they are advancing them, unless their estimate of the costs and benefits of that policy changes. In particular, they are not going to abandon the policy to comply with America's vision of how a great power should act. They reject that vision.

Now what are America's interests? They are, in brief:

- Freedom of trade and travel in the region, on equal terms with other nations, including China;
- Upholding the norm-based international order which reflects American values, preserves the peace, and under which the United States and much of the world has prospered.
- Fulfilling America's de jure and de facto treaty commitments to Japan, the Philippines, Taiwan, and Australia. One of the pillars of American foreign policy since the end of World War II is gathering partners around the world, both to share the burdens of security and to validate American leadership. Abandoning those alliances in Asia would undermine our alliance structures around the world; it would mean, as a practical matter, the collapse of America's security architecture, and the end of stability in vital regions of the globe.

The object of the United States should be to protect its vital interests using means that have a high probability of success and as low a probability as possible of armed conflict, or at least escalating armed conflict. The key to a successful policy is to understand that America is in a strategic competition with China, and probably will be for a long time. Many people in this country hoped that China would not move in the direction of competition – that the CCP would not see its relationship

with the United States as a zero sum game. It may be possible to channel them into a more cooperative relationship over time, but not if they see themselves as winning the competition with the United States.

America must commit itself to competing effectively with China. That means firmly deterring Chinese aggression and coercion without provoking them unnecessarily. The Chinese are a proud people with a long and distinguished national history. Our leaders should be respectful of that and should insist on respect in return.

As an example, if the United States sends a representative to an international conference, and a Chinese general spends 20 minutes voicing the most outlandish distortions about American policy in Asia, there should be an appropriate response. If the United States invites China to join our annual allied RIMPAC naval exercise in the Pacific, and the Chinese decide to join it but send a vessel to collect intelligence – thereby sticking their thumb in America's eye – there should be an appropriate response.

Currently American policy has been to vigorously pursue so called "mil-to-mil" exchanges with China, where senior American officers engage in talks with their Chinese counterparts. If the object is to reduce the risk of accidental military confrontations, or to learn something of value about Chinese operations, the exchanges are unobjectionable. But if the motivation is the belief that talking with Chinese military officers will change China's policy in the region, the exchanges evidence weakness, a patronizing attitude that undermines deterrence, and a naïve lack of understanding of the nature and goals of the CCP leadership.

The Obama Administration has pursued a "rebalance" to the Pacific in response to Chinese aggression. The rebalance entails shifting military forces to the western Pacific, firming up America's alliances there, and presenting China with a united diplomatic and military front. It's the shell of a good policy but is failing for want of power. America cannot shift forces it does not have, and it's hard to maintain the confidence of allies who see what everyone outside of Washington sees: that America is becoming weaker while China grows stronger.

When Barack Obama took office, America's armed forces were already stressed by years of fighting and underfunding, particularly of the procurement

accounts. The force was smaller than it had been in the 1990s – at a time of relative peace around the world – and all of the services were desperately in need of recapitalization.

The Obama Administration cut defense funding by approximately $400 billion during its first two years. Then in the spring of 2011, Secretary Bob Gates proposed a ten-year budget plan with very modest yearly increases in the defense topline. However, within a few months thereafter, the President proposed another $400 billion dollar cut in his own budgets, and shortly after that, the President signed the Budget Control Act and conditional sequester that resulted, beginning in 2013, in a trillion dollar cut to Secretary Gates' 10-year defense plan.

It was unprecedented for a president to recommend such large reduction in his own defense submission, and unprecedented for the president and Congress to cut the defense budget by so large amount *without any analysis* whatsoever of the effect on the armed forces.

At the time, Secretary of Defense Leon Panetta predicted that the cuts would be "disastrous", and they were. All of the forces have shed force structure and cut modernization plans. The upshot is that the Navy is now smaller than at any time since 1917, the Army is declining in size and will soon reach pre-WWII levels, and the Air Force is smaller, and flying older aircraft, than at any time since the inception of the service. In addition, the day-to-day readiness of all the services has been adversely affected.

Passage of the Budget Control Act of 2011, and the fact that it remains the law to this day, signals to CCP leaders that the United States is not able or willing to assign additional naval and air forces to the region – to counter China's military buildup – and thus is not prepared to sustain its leadership role in the Western Pacific.

To sustain a successful policy in the Western Pacific, the United States must increase the presence of its armed forces in the Western Pacific, in a way that effectively counters the asymmetric strategy of the Chinese and therefore effectively deters their coercive tactics. That will not be possible without a major increase – similar to the Reagan-era buildup -- in the overall strength of America's armed forces;

the United States cannot base or rotate forces into the Western Pacific if those forces do not exist.

The exact nature of that buildup is beyond the scope of this chapter to discuss. Readers who want to review what a plan might look like – and reasonable people can certainly disagree on the specifics – should read an October 2015 report issued by the American Enterprise Institute, "To Rebuild America's Military."[3]

The object of such a buildup would be to give American presidents options in the event of a regional crisis, to convey political will, to reassure allies, and to underpin diplomatic efforts. Specifically, the United States needs the ability to respond to coercion effectively without setting off a chain of escalating armed conflict.

Suppose, for example, that China moves to take effective control of a reef belonging to the Philippines (as they have already taken control of the Scarborough shoal). The Philippines is an ally and treaty partner of the United States. If the only effective response available to the President would require attacking China's fleet, or its missile forces on the mainland, it is highly unlikely that he would approve such an escalatory option; and knowing that, the existence of the option would be less likely to deter China's leaders in the first place

But if American naval forces were available in quantity at the site of the confrontation, they could protect the contested reef and escort Filipino vessels in resupplying it. The confrontation would be tense, but not necessarily escalatory. Much as President Kennedy was able to succeed during the Cuban missile crisis because he had the naval forces to blockade Cuba rather than bomb it, deterrence in the Western Pacific requires the presence of sufficient American forces to create options which are effective but non-escalatory.

In fact, an American military buildup would immediately have a deterrent effect on Chinese leaders; it would signal to the whole region that America intended to keep its commitment to its allies and continue to play a leadership role on behalf of our mutual interests. In this sense, defense policy *is* foreign policy; adversaries and

[3] Thomas Donnelly et al., *To Rebuild America's Military*, American Enterprise Institute, October 7, 2015, https://www.aei.org/publication/to-rebuild-americas-military/.

allies alike understand that American determination to sustain its strength is strong evidence of American resolve to protect its interests and allies.

If a year from now the new American president announces that he or she is changing the outgoing administration's budget and asks for a double-digit increase in the defense budget – if he or she proposes ending the defense sequester, stopping the reduction in the end strength of the U.S. Army, increasing the procurement of 5th generation fighters and increasing naval shipbuilding by 50% or more -- and if such proposals were received favorably by Congress, China's leaders would immediately take notice that henceforth the United States intended to reinforce the rebalance policy with real power.

Of course, rebuilding American military presence in the region is not all that should be done. Making the rebalance successful will also require a broad and strong bipartisan consensus in support of it, and parallel diplomatic and political efforts designed to expose China's strategy, strengthen America's partnerships in the region, and shape the international narrative regarding Chinese aggression in East Asia and the corruption and human-rights abuses of the Chinese regime at home.

One intriguing idea advanced by American Enterprise Institute scholars Dan Blumenthal and Michael Mazza would be to initiate a process designed to resolve the outstanding disputes among various countries in the South China Sea.[4] To this point, the United States has urged that the disagreements be resolved through negotiations, but the government has taken no position on what the outcome should be. That is appropriate, but the United States could show leadership by approaching the claimants, multilaterally or bilaterally depending on circumstance, and attempting to negotiate an agreeable resolution. China could be invited to participate, but should be informed that whether they participated or not, the United States intended to pursue negotiated settlements and would endorse the outcome of the talks.

As I discussed above, the rebalance to Asia is the shell of a good policy, but it failing for want of power. Unless that is remedied, the rebalance could have the opposite of the intended effect; it could present the United States as the obstacle to

[4] Daniel Blumenthal and Michael Mazza, "A New Diplomacy to Stem Chinese Expansion", *Wall Street Journal*, June 10, 2015, http://www.wsj.com/articles/a-new-diplomacy-to-stem-chinese-expansion-1433952079.

China's ambitions and its perceived vital interests, without also presenting the power and determination necessary to deter aggression.

I call this "provoking without deterring", and it can be extremely dangerous. It could lead to a disastrous miscalculation on the part of the Chinese; if the balance of power continues to shift in their direction, it could embolden them to take a serious risk in the region. Xi Jinping is a dynamic and ambitious leader. If he adheres to the past practice of the CCP, he will retire from leadership after a single ten-year term, which will end in 2023; he may well want to make a decisive move to achieve China's ambitions before then, if he believes that the balance of power – what the Soviets used to call "the correlation of forces" -- has moved even more in China's favor.

No American should be afraid of a long-term competition with China. It's going to happen in any case; for the reasons already discussed, the CCP has interests which it considers vital, which it will certainly continue to pursue, and which are inconsistent with the interests and long-standing regional policy and posture of the United States.

Judged in the broadest sense, the United States is considerably stronger than China under the CCP. Most of the countries in the region are either allies or potential American allies; except for North Korea, the other nations of East Asia see a conjunction, on the strategic level at least, between American interests and their own, and they would vastly prefer that the United States rather than China be the dominant regional power. The domestic challenges facing the United States are substantial, but they are small compared to the challenges facing China: it has no private banking system, no legal system, no reliable tax system, a tremendously unbalanced economy, a huge real estate bubble, a debt equal to 250% of GDP, shrinking foreign reserves, widespread environmental degradation, and a government which has no firm basis for popular legitimacy.

If America uses its strengths, consistently and wisely, there is every reason to believe that it can protect its interests and allies in a way that preserves peace and stability in the Western Pacific. The alternatives are to abandon the region to China or continue the current policy of provoking China without adequate deterrence.

In the late 1930s, the United States also confronted a rising Asian nation with pretensions of hegemony, and as now, America neither got out of the way of that nation nor sustained the regional power necessary to protect its interests while deterring armed conflict. That episode in history did not end well. America's new President should resolve that this time the outcome will be different.

A Turbulent China Shakes the World

By Gordon G. Chang

The regime that was supposed to own the century may not survive the decade. The People's Republic of China is now trapped in slow-burning economic and financial crises that are shaking the country.

China's difficulties are contributing to troubling changes in its politics, and those political changes are already affecting Beijing's external policies, making them far more provocative.

Whether or not the Communist Party manages to get beyond the current crises, China will pose the single greatest threat to the United States and the international system.

Although the global narrative about China is evolving, America and other nations are not prepared for the consequences of what is occurring inside the Chinese state. After all, China is perhaps the world's fastest-changing society today, and that means the country emerging from this period is bound to be very different than the one we see today.

Two Historic Transitions in China

Most people believe the history of the People's Republic of China can be divided into two broad stages, one dominated by founder Mao Zedong and the other begun by his successor, Deng Xiaoping.

Virtually every analyst and policymaker will tell you China is still in the second one. Yet change, driven primarily by economics and politics, in the past half-decade has been so fundamental and transformative that the country has passed into a third stage, an especially turbulent and troubling one.

The transition from the first to the second era—from Mao to Deng—was easy to identify, even at the time. Mao died, and two years later Deng was running things. As Deng consolidated control, China passed from its Maoist beginnings to an era of "reform and opening up."

Now, however, China is regressing and closing down. This critical transition from the second to the third era began toward the end of the rule of Hu Jintao, the predecessor to the current leader, Xi Jinping, president of the Chinese state and, far more important, general secretary of the Communist Party.

The Distressing State of the Economy

To understand what is happening in China now, we begin with the economy. The economy has been the motor of the country's rise, but it is now looking like the engine of its fall.

In the so-called reform era, annual growth of gross domestic product averaged about 9.9%. The days of heady growth are over, however. The country, according to official figures, was last in double-digit territory in 2010, when the economy grew 10.4%. In all probability, growth that year was in excess of that number, perhaps by a full percentage point.

Since then, there has been a rapid decline in growth rates. The official National Bureau of Statistics, NBS, reported GDP grew 6.9% in 2015.

Many believe this official number is far too high. Citigroup's chief economist, Willem Buiter, in the middle of 2015 called Beijing's growth data "mendacious."[5] Buiter suggested the economy was expanding around 4%, and there is a consensus forming that he is right. The Conference Board's Harry Wu and Angus Maddison for instance, put 2015 growth at 3.7%.[6]

Growth could be even lower, however. In the middle of last year, a well-known China analyst was privately noting that people in Beijing were talking 2.2%, and there are indications the economy grew at an even slower pace, perhaps 1%.

The headline GDP number is not consistent with various indicators, including other official data. For example, the best indicator of Chinese economic activity remains the consumption of electricity, and in 2015 electricity consumption

[5]Sangwon Yoon, "China Will Respond Too Late to Avoid Recession, Citigroup Says," Bloomberg Business, August 27, 2015, http://www.bloomberg.com/news/articles/2015-08-27/china-will-respond-too-late-to-avoid-recession-citigroup-says.

[6]Harry Wu and Angus Maddison, "The Conference Board Global Economic Outlook, 2015-2025," Conference Board, https://www.conference-board.org/data/globaloutlook/index.cfm?id=27451.

increased, but only by 0.5%. Incidentally, electricity generation for the year was down 0.2%, the first drop since 1968.

Two other important indicators show there was hardly any growth last year. First, imports, in dollar terms, were down 14.1%, a clear sign of troubles in both the manufacturing sector and in consumption.

Even more damning is price data. China officially is in a deflationary period. According to NBS, nominal growth last year of 6.4% was well below real—price adjusted—growth of 6.9%. And deflation in the fourth quarter was particularly ugly: nominal 5.8%, real 6.8%. It is simply not possible to have, at the same time, a robust expansion and deepening deflation.

Beijing says China turned from deflation to inflation in the first quarter of this year. That is unlikely to be true, especially because the reported growth rate fell in the first quarter to 6.7%. Chinese authorities are now just making up numbers to meet announced targets.

In one sense, it does not matter how fast China is growing. The important point is that Chinese leaders no longer have the ability to create sustainable growth, in other words, to prevent the downward trajectory of the economy.

Six reductions in benchmark interest rates since November 2014 and five reductions of the bank reserve-requirement ratio since February 2015 have had no noticeable effect. This monetary stimulus is tapped out because there is a fundamental lack of demand for money.

Fiscal stimulus also appears to be ineffective. Fiscal spending, a good measure of the government's overall simulative efforts, accelerated as 2015 wore on. It was up 25.9% in August, 26.9% in September, 36.1% in October, and 25.9% in November. The Finance Ministry did not report a December number but did announce that for the year as a whole such spending was up 15.8%, confirming that stimulus skyrocketed as the year progressed—and as GDP growth trended down.

Moreover, even massive amounts of new credit and government spending in the first quarter of this year could not prevent the reported growth rate from declining.

And two other growth strategies came a cropper: the reckless promotion of share prices beginning in the fall 2014, intended to create a wealth effect and to help enterprises pay off debt with new stock, and the botched devaluation of the renminbi beginning mid-August 2015, which tended to help exporters and producers for the domestic market.

Economy Headed for Contraction

As a result of Beijing's failed policies, the economy is headed for contraction as Chinese leaders can, at best, slow the pace of descent, not change course. Even the implementation of structural economic reform, something on everyone's wish list, has now been delayed too long to avoid a recession or worse. Meaningful reform takes years to have a positive effect, and China, in reality, is just months away from beginning a long period of negative growth.

Chinese leaders continually talk about economic reform—as they did after the Communist Party's Third Plenum in November 2013 and after the Fifth Plenum in October of last year, where the topic was the 13th Five-Year Plan—but they have implemented little of it. Moreover, what little that has been put in place has often been more for show than substance.

Worse, Xi Jinping has, on balance, taken the country backward during his tenure, among other things closing off the Chinese market to foreigners; recombining already large state enterprises back into formal monopolies; increasing state ownership of state enterprises, reversing the partial privatization of earlier years; and shoveling more state subsidies to favored market participants. Xi, with draconian measures, also strangled financial markets beginning in early July of last year, to keep share prices high and currency values elevated. And on top of this, Xi is pushing a number of national security laws and regulations that effectively prevent foreign companies from doing business with state enterprises and governmental units.

His signature initiative, encapsulated by the phrase "Chinese dream," contemplates a strong state, and a state-dominated China does not sit easy with the notion of market-oriented reform. Unfortunately for China, there are no economic solutions that are possible within the political framework Xi will not change.

China needs growth now primarily because government deficit spending is adding to already worrisome debt woes. McKinsey Global Institute pegged the country's debt-to-GDP ratio at a precarious 282% at mid-2014,[7] but the number is surely higher than that now. In reality, the ratio at this moment could be somewhere in the vicinity of 350%—the number George Soros mentioned in January in Davos[8]—or 400%, the number Andrew Collier of Orient Capital Research in Hong Kong calculated at around the same time. China, as an increasing number of analysts think, is headed to an impossible-to-avoid debt crisis.

Jonathan Anderson of Emerging Advisors Group puts the "threshold" for the "initial potential crisis" at "around five years,"[9] but months could be a better prediction. "They absolutely have no room left for further debt accumulation," says Rodney Jones of advisory firm Wigram Capital.

Observers make the argument that, despite everything, we don't have to worry because Beijing technocrats dictate outcomes and they would never permit a crash. Chinese technocrats do dictate outcomes, but that is precisely why their country is now heading to catastrophic failure. Because China's political leaders have the power to prevent corrections, they do so. Because they do so, the underlying imbalances are becoming larger. Because the underlying imbalances are becoming larger, the inevitable correction must now be severe.

Severe Adjustment Coming

Downturns, which the Communist Party hates because it is politically insecure, are essential. They allow adjustments to be made while they are still relatively minor. The last year-on-year contraction in China's gross domestic product,

[7] Richard Dobbs, *et al.*, "Debt and (Not Much) Deleveraging," McKinsey Global Institute, February 2015, http://www.mckinsey.com/insights/economic_studies/debt_and_not_much_deleveraging.

[8] Ambrose Evans-Pritchard, "Hysteria Over China Has Become Ridiculous," *Telegraph* (London), January 27, 2016, http://www.telegraph.co.uk/finance/economics/12123602/Hysteria-over-China-has-become-ridiculous.html.

[9] Tom Mitchell, "The Ugly Subtext Beneath China's Two-Track Economy Tale," *Financial Times*, January 17, 2016, http://www.ft.com/intl/cms/s/0/bb494388-bb9b-11e5-bf7e-8a339b6f2164.html#axzz3xVy5B1wQ.

according to the National Bureau of Statistics, occurred in 1976, the year Mao Zedong died.

So China's next downturn will surely be historic. Chinese leaders will prevent adjustments until they no longer have the ability to do so. When they no longer have that ability, their system will go into free fall. When it goes into free fall, the economy will collapse.

That may sound extreme, but perhaps not to the global financial community. There are dozens of hedge funds that are shorting the Chinese currency at the present time.

And the Chinese people may be even more pessimistic than currency speculators. A Barclays study released in September 2014 shows that a stunning 47% of China's rich planned to leave their country within five years.[10] Given the evident deterioration in the economic situation since then, probably even more Chinese are thinking of moving elsewhere now.

Despite the darker views, almost all analysts through the end of last year said there was nothing to worry about because Beijing had plenty of foreign exchange reserves. That theme is heard less often as the reserves have fallen more than most people thought possible. The State Administration of Foreign Exchange, the central bank's custodian of the reserves, reported that the reserves dropped $512.7 billion in 2015, and it's possible the number is even higher than that because of deliberate underreporting. There is also a concern that Beijing's reserves are not as liquid as represented to be.

In any event, China is fast heading to the point where its reserves are not adequate. Even if Beijing has accurately reported its holdings of foreign cash, the reserves are just months away—perhaps as few as five—from reaching what is considered a red-line level.

Beijing found itself in this predicament because of unprecedented capital outflow. The Washington, D.C.-based Institute of International Finance estimated

[10] Dexter Roberts, "Almost Half of China's Rich Want to Emigrate," Bloomberg Business, September 15, 2014, http://www.bloomberg.com/bw/articles/2014-09-15/almost-half-of-chinas-rich-want-to-emigrate.

net outflow last year to be $676 billion. Beijing-based J Capital Research puts the number at $911 billion, and Bloomberg's estimate is $1 trillion.

People still think a "soft landing" is possible, but by now the odds of a severe adjustment—something on the order of 1929—are increasing fast.

Political Turmoil in the Communist Party

The economy is not the Communist Party's only problem at the moment. China's economic difficulties are deepening while the country's political trauma continues. In short, the country has yet to complete an historic leadership transition that has been changing decades-old patterns of governance.

Deng Xiaoping's contribution to Chinese communist politics was to reduce the cost of losing political struggles—often death in Maoist times—thereby reducing the incentive to fight to the end and tear the Party apart.

Xi Jinping, according to most analysts, quickly consolidated his political position after becoming the Party's general secretary in November 2012. He did this, most notably, with his so-called anti-corruption campaign.

There is, however, evidence that the transition has been far from "smooth," something evident from Xi's wide-ranging prosecution of both high- and low-level officials, "tigers" and "flies" in Beijing lingo. New Chinese Communist leaders have always engaged in some housecleaning, but Xi's efforts have been unprecedented in scope and duration. The campaign, some believe, threatens the basis of Party rule by "deconstructing" the web of patronage relationships that has, over the course of decades, kept the ruling organization in power.

For almost four decades, powerbrokers tried to maintain a delicate balance among the Party's competing and shifting alliances, factions, groups, and coalitions. Xi, however, has sought to eliminate factionalism and has thereby roiled the political system, breaking decades-old norms designed to ensure stability. As one of his political allies said, his motto is "You die, I live."[11]

[11] John Garnaut, "China's Power Politics," *New York Times*, August 11, 2014, http://www.nytimes.com/2014/08/12/opinion/chinas-power-politics.html?partner=rss&emc=rss&_r=1.

Xi, in many ways, is going back to Mao's strongman system. For instance, one commentator said recently that China's supremo is "reintroducing fear as an element of rule for the first time since the Cultural Revolution."[12] Therefore, his unprecedented actions look like they mark the end of a quarter century of calm, a time that permitted China to recover from, among other things, Mao's 27 years of calamity and Deng's 1989 Tiananmen massacre.

At this moment, the Communist Party appears headed to another round of debilitating leadership struggle, something evident from the series of rumors of coup plots and assassination attempts, especially in the first months of 2012, on the eve of Xi taking power, and again in 2014.

These rumors, for the most part, were false, but clearly something was—and still is—amiss in elite circles. The fact that terrified and desperate political players spread stories of armored cars in the center of Beijing and gunfire in the Communist Party leadership compound of Zhongnanhai means groups are trying to destabilize Xi's regime. Xi, in short, has pushed opponents so far they believe—probably correctly—that they have no choice but to fight.

Xi's relentless campaign has been generally viewed as proof he dominates the political landscape. Yet purges, conducted in the guise of an anti-corruption campaign, are signs of continued weakness of China's leader, not his strength. If Xi Jinping were as strong as many believe, why would there be need for more purges?

Why is Xi purging opponents with such determination? Among other reasons, he came to power in an unusual transition. His elevation was all the more remarkable because he became China's supreme leader without the support of any faction he could call his own. He appealed to all factions, in large part because he had no faction. Xi was, in short, the least unacceptable choice.

Not being identified with any faction was the right way to climb to the apex of power, but, once there, he felt vulnerable without a faction, especially in a system riven with them. So Xi set out to create a grouping of his own with the military as the core of his support. And at the core of Xi's military support are the officers of what

[12] Daniel Twining, "The People's Republic of Uncertainty," *Nikkei Asian Review*, January 24, 2016, http://asia.nikkei.com/Viewpoints/Viewpoints/The-People-s-Republic-of-uncertainty.

was, before the recent reorganization of the People's Liberation Army, the Nanjing Military Region.

Remilitarization of Politics

Xi, also chairman of the Party's all-powerful Central Military Commission, is thought to control the People's Liberation Army. Nonetheless, military officers wield great influence over him.

Why? Xi depends on the generals and admirals for his political support. He cannot say "no" to senior officers because they are the closest thing he has to a political base, which is sometimes called the "Zhejiang faction," a reference to Xi's posting to that province before his elevation to the top spot.

The primacy of the military has implications. From all outward appearances, senior officers are already playing an expanded role in Beijing. For instance, Hu Jintao, a weak leader, was able to resist military pressure to declare an East China Sea Air-Defense Identification Zone. Such a zone was in fact declared within a year of Xi becoming general secretary, an indication that flag officers began to wield influence soon after Comrade Xi took over.

The rise of the military did not start with Xi's ascension. In fact, it began much earlier, with the political jockeying during the end of the tenure of Jiang Zemin, Hu's predecessor. Yet the influence of flag officers has continued to grow, and in Xi's China generals and admirals are making their "military diplomacy" the diplomacy of the country.

The remilitarization of politics and policy is pushing China in frightening directions. "China's military spending is growing so fast that it has overtaken strategy," said Huang Jing of Singapore's Lee Kwan Yew School of Public Policy. "The young officers are taking control of strategy and it is like young officers in Japan in the 1930s. They are thinking what they can do, not what they should do."[13]

At this moment, China's officers, from generals to lieutenants, are thinking about what they want, and as a result they have become dangerous, arrogant, and

[13] Ambrose Evans-Pritchard, "China's Young Officers and the 1930s Syndrome," *Telegraph* (London), September 7, 2010, http://blogs.telegraph.co.uk/finance/ambroseevans-pritchard/100007519/china%E2%80%99s-young-officers-and-the-1930s-syndrome/.

bellicose. By their own admission, they are spoiling for a fight. And in a time of transition, perhaps no civilian leader—maybe not even Xi—is in a position or willing to take a risk to tell the top brass what to do.

Xi's "impulsive style" in foreign policy, highlighted by the *Wall Street Journal* in June of last year, suggests that Chinese policy is losing coherence,[14] and one reason may be that generals and admirals are now so strong that they can do what they want, with minimal—or in some cases no—oversight. Therefore, we cannot discount the possibility of disunity complicating both policymaking and governance.

China's Belligerence

The implications of these internal changes are obviously large because, for the most part, the flag officers do not want a closer relationship with the international community. On the contrary, their brand of militant nationalism is creating friction in an arc of nations from India in the south to South Korea in the north.

Beijing, for instance, is trying to appropriate for itself the international waters of the South China Sea. That brings China into a zero-sum match with another party, the United States. If there has been any consistent American foreign policy over the course of two centuries, it has been the defense of freedom of navigation. China, however, is trying to drive America off the high seas and out of international airspace.

China, therefore, is no longer a status quo power. It is not promoting worldwide revolution as it did in the early years of the People's Republic, but it is trying to fundamentally change the existing international order.

And Beijing is not just being assertive; its foreign policy has now become counterproductive. In the past, Beijing punished neighbors. Chinese leaders, however, were always smart enough to direct their anger at just one or two targets to make sure they got what they wanted. And many times they were in fact successful.

Today, Beijing is taking on many others all at the same time. The Party is lashing out, and that is not a good sign. If nothing else, it betrays a lack of strategic

[14] Andrew Browne, "The Whiplash of Xi Jinping's Top-Down Style," *Wall Street Journal,* June 23, 2015, http://www.wsj.com/articles/the-whiplash-of-xis-top-down-style-1435031502.

thinking. So we need to be concerned that Chinese leaders are now acting according to a logic that the rest of the world is not familiar with.

These days, Beijing seems aggressively determined to pursue self-marginalizing, self-containing, and ultimately self-defeating policies. As a result, Beijing is suffering one foreign policy setback after another, something evident from the loss of allies, especially in Sri Lanka, Burma, and most recently Taiwan. At the same time, China's actions are resulting in the formation of a coalition against it, comprising, most notably, of India, Vietnam, the Philippines, Japan, Australia, Singapore, and the U.S.

Why is China not pulling back when it clearly would be in its interest to do so? There are two points, both rooted in the country's new third era, to consider. First, for more than three decades—China's second era—the primary basis of legitimacy of the Communist Party was the continual delivery of prosperity. And without prosperity, the only remaining basis of legitimacy today—the third era—is nationalism. An increasingly virulent nationalism is pushing Beijing into taking worrying actions.

Second, the emergence of the military in the political system means that some of the most bellicose elements in Beijing are now calling the tune. And they are supported by Xi. Not since Mao has China had a leader as ambitious. And Xi's ambitions expand far beyond the areas currently within the boundaries of the People's Republic.

Reaction of the International Community

Other than the North Koreans, who somehow have Beijing's number, everyone is struggling to find the magic formula for good relations with China. Since Nixon's 1972 trip to Beijing, the virtually unanimous answer has been "engagement." "Taking the long view," Nixon famously wrote, "we simply cannot afford to leave China forever outside the family of nations, there to nurture its fantasies, cherish its hates, and threaten its neighbors."

As a nation, we made a bet that China would become a true partner rather than another Soviet Union. It was the grandest wager of our time.

In China's second era, the wager on engagement seemed to work, but in the third era it has become a losing bet. In recent years, it has become clear that we have, through engaging China, helped create an economically powerful and belligerent state. Now, our policymakers have yet to admit that more than four decades of engagement of the Communist Party have not produced desired results. Not surprisingly, most foreign policy establishments in Washington and other places have spent the last half decade trying to ignore what was happening in Beijing.

Ignoring China's actions made matters worse. In the first part of 2012, for instance, Chinese vessels swarmed Scarborough Shoal in an attempt to wrest it from the Philippines. Washington quickly brokered an arrangement in which both Beijing and Manila agreed to withdraw their vessels from Scarborough, a feature in the South China Sea close to Philippine shores.

Only Manila complied. Washington did nothing to enforce the agreement it had sponsored and so let the Chinese vessels seize the shoal. The apparent hope was that if the international community ignored this act of aggression, Beijing would be satisfied with its conquest.

Yet the Chinese military, emboldened by success, just ramped up attempts to seize more territory, from both the Philippines—Second Thomas Shoal—and Japan—the Senkaku Islands. Worryingly, Chinese media also began talking about claiming Japan's Okinawa and the rest of the Ryukyu chain as well.

China's actions in the last half decade are reminiscent of the events leading up to the invasion of Poland in September 1939. The nature of the regimes is different, of course, but the dynamic of aggression is similar.

A policy better than appeasement—engagement now resembles Neville Chamberlain's now-derided approach — is Taro Aso's. In late 2006, when he was Japan's foreign minister, Aso proposed an "arc of freedom and prosperity" for Asia. Then, his concept of a coalition of democracies went nowhere because regional leaders were optimistic about China enmeshing itself into the international system and becoming a supporter of the global commons.

Relationships Moving Forward

Now it should be clear that, except perhaps in limited areas, long-term cooperative relations with Beijing are not possible. The fundamental problem is that China is not stable, so its leaders, for various reasons, are in no position and no mood to deal with their counterparts in other capitals on a good-faith basis.

We tend to think there are always solutions to every problem, but in the case of China there do not appear to be any, other than deterrence. And because we can only deter, American policymakers need to say out loud that "containment," a word Washington cannot utter in connection with China, is an option. At the moment, however, the tired—and feeble—language of cooperation is still heard.

Perhaps Washington policymakers should read Confucius, especially about what the sage called the "rectification of names." "The beginning of wisdom," he wrote, "is to call things by their proper name." If we cannot label Chinese actions "aggression," for instance, we have little hope of maintaining peace in the region.

As China's ambitions expand rapidly, we can't even get out of its way. In the third phase of the People's Republic, our assumptions about a peaceful, prosperous China look obsolete. And as that country changes, so too must our policies.

Recommendations

What to do about China? In short, we need to make declarations, reverse gains from aggression, work with friends, impose costs, and change the terms of contact.

- We must change what we say to Chinese officials and how we say it. We are afraid to anger Beijing, so we speak in soft tones in public. Chinese leaders do not see this as a signal of cooperation. On the contrary, they sense fear and press what they perceive to be their advantage. This, naturally, has reinforced the aggressive tendencies in China's political system.

  We need to make declarations to show we are confident in ourselves and unwavering in defense of our principles. This is a particularly good time for everyone in the American capital to read up on Ronald Reagan.

- We need to reverse China's gains from territorial aggression. Chinese admirals, for instance, need to see the U.S. Navy around Scarborough Shoal until they decide to go home.

The international system may be sturdy, but it can be taken down quickly when aggressors are allowed to keep territory they have seized. Nothing will be as effective in restoring stability in East Asia as a return to Philippine control of Scarborough.

Do we risk armed conflict in forcing the Chinese to abandon the shoal? Yes, but American leaders, employing policies that sounded good to the ear, let the situation drift for so long that there are no good options left.

Remember, the choice is not confrontation versus no confrontation. We allowed China to take Scarborough. Did that end confrontation? No, it just meant China increased its ambitions and created confrontations elsewhere.

The choice is not risk versus no risk. The choice is which awful risks we will assume. If we do nothing now, we will only be creating the conditions for great-power conflict in the future.

And with Russia increasingly in China's corner, this could be America's greatest struggle. The United States has not faced two peer competitors since the end of the Second World War or a united China and Russia since the end of the 1950s, but now we do. The combination of the Dragon and the Bear is going to change the world in ways we can only begin to imagine, and none of them will be good.

- We should be strengthening our commitments to our friends in the region. Simply stated, we should work and trade with those who share our goals and our values. Taro Aso, in short, was right.
- We need to impose costs on China for unacceptable conduct, like the hacking of American businesses for commercial gain and the cyberattacking of the institutions of our free society, such as the media, foundations, charities, and advocacy groups. Only when Beijing has to bear burdens greater than the benefits it receives will it stop this and other destructive conduct.
- We need to change the terms of contact with China. There is a deep-seated feeling that contact is necessary for good relations. The opposite may be the case.

  Need proof? As the number of contacts with China has dramatically increased this century, ties have gotten worse. Obviously, talking more has not been helping.

  Specifically, we should break off some of the mil-to-mil contacts that are inappropriate. China's military officers do not distrust us because they have insufficient contact with us. They distrust us because we stand between them and their outsized ambitions.

If we talk less, Beijing's leaders will get the message. And we will stop feeding their already inflated notions of self-importance.

- Instead, we should engage the Chinese people. The regime, after all, may not last long. If this assessment is correct, and there are many reasons to believe it is, we need to have good relations with those who will next lead China.

  Many say the Chinese people are not important actors in their own society, that they are not ready to govern themselves. That's not true. In 2008, just before the Beijing Olympics, my wife and I went back to Rugao, my dad's hometown, a dusty backwater in Jiangsu province north of the Yangtze River. We wanted to find out what people thought about the extravaganza, but no one wanted to talk about the event, which was derided as "the government's games."

  Instead, people asked my wife and me about how the American political system worked and who would win the presidential election of that year. They wanted to know everything we could tell them about John McCain, Barack Obama, and the constitutional concept of checks and balances.

  One day, the Chinese people will not only have a greater say in their lives, they will determine their own fate. We should, therefore, get to know them better.

We must change our course not only for ourselves, not only for future generations of Americans, but for people everywhere—including China—who share the principles and values we defend.

CHINA, UNRESTRICTED WARFARE, AND THE CHALLENGE TO AMERICA

By Kevin D. Freeman, CFA

Since the People's Liberation Army (PLA) Press published *Unrestricted Warfare* in February 1999, China has enjoyed an almost unprecedented rise in fortune relative to the world in regard to economic, military, and global stature. Upon closer examination and in hindsight, a good portion of this rise may be attributable to following the PLA strategy.

The basic premise of Unrestricted Warfare (UW) is that, in a global age, everything must be considered a matter of warfare. This is made quite clear in the final words in the concluding chapter of the book:

> Although the boundaries between soldiers and non-soldiers have now been broken down, and the chasm between warfare and non-warfare nearly filled up, globalization has made all the tough problems interconnected and interlocking, and we must find a key for that. The key should be able to open all the locks, if these locks are on the front door of war. And this key must be suited to all the levels and dimensions, from war policy, strategy, and operational techniques to tactics; and it must also fit the hands of individuals, from politicians and generals to the common soldiers.
>
> We can think of no other more appropriate key than "unrestricted warfare."[15]

Essentially, this is a total warfare construct. Everything is a battle space, whether trade negotiations, currency exchange, employee relationships, fiscal policy, or R&D. As a result, everything must therefore be viewed through the lens of Unrestricted Warfare. The Chinese authors indicated things like "a single, manmade stock market crash" is a "new concept weapon." They defined George Soros (famous for currency attacks) as a "financial terrorist." And they declared that a computer

[15] Qiao Liang, Al Santoli, and Xiangsui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America*. English Translation. (Panama City, Panama: Pan American Pub., 2002), 191.

hacking can exert more influence than a nuclear bomb. Overall, they declared, "that there is nothing in the world that cannot be a weapon." And while China appears to have fully grasped this thinking, the Chinese authors explained why they believed Americans would not be able to grasp the changes to warfare:

> However, the Americans have not been able to get their act together in this area. This is because proposing a new concept of weapons does not require relying on the springboard of new technology; it just demands lucid and incisive thinking. However, this is not a strong point of the Americans, who are slaves to technology in their thinking. The Americans invariably halt their thinking at the boundary where technology has not yet reached.

Unfortunately, this appears to be true as the American defense and intelligence establishment often disregard the concept of total war. Those charged with monitoring economic relationships, for example, tend to look for economic motives and frequently miss the geostrategic implications. Too often, they assume that China would never make a move that might be detrimental to their economy even if that move might prove crippling to a perceived enemy. Those who might be inclined to question Chinese motives, however, are too often placed in narrow silos of thought that prevents them from recognizing economic signals because they are not in their "swimming lanes."

Since 1999, history has demonstrated that Unrestricted Warfare is not simply a theory for the Chinese government. It has clearly been their action plan over the past two decades and if successfully followed as outlined could end in the collapse of the United States without a direct military conflict. This is not to say that China is immune from the likely devastating blowback that would happen. In fact, the repercussions may be even worse for China than America in many ways as the Chinese economy is more vulnerable. But the longer-term negative ramifications to society were apparently not considered carefully when China adopted a "one-child policy." Yet this did not prevent the enforcement of such disastrous social planning that will negatively impact the nation for decades to come.

The fact is that China has been implementing Unrestricted Warfare in spite of the willful blindness, disbelief, and ignorant arrogance prevalent within much of

our defense and intelligence leadership. Granted, China is not a monolith. There are various power factions such as the business community, the PLA, and the Communist Party that at times compete against one another. When their interests align, however, the direction is absolute. Unfortunately, our analysts tend to overemphasize the influence of the business community due to Western-thought bias. They assume that individuals and nations tend to act rationally as defined by economic self-interest, typically with a shorter time horizon. Such is not the case for China as the drive for geopolitical domination is far greater than for short-term economic returns. Chinese planners view five-year plans as short term.[16] They tend to think in terms of decades and centuries rather than quarters or years.[17] Perhaps this is the benefit of a 4,000-year old civilization.[18] And, while the goal is to dominate through economic means, the Chinese are not content to play by Western rules. Rather, they are determined to win long-term dominance through Unrestricted Warfare.

The Chinese strategy has been extraordinarily effective, especially in regard to propaganda, public disinformation, and influence campaigns. The vast majority of the Washington establishment considers China a basically benign power seeking to join the Western international framework through growth and cooperation. Perhaps no one understands this better than Michael Pillsbury as noted in a recent NY Post article on his book, *The Hundred Year Marathon*:

> …Michael Pillsbury, an expert on China who has worked with every US president since Nixon and has, he writes, "arguably had more access to China's military and intelligence establishment than any other Westerner," …
>
> In a sense, the new book "The Hundred-Year Marathon" is Pillsbury's mea culpa. He readily admits that, as a key influencer of US government

[16] "Why China's five-year plans are so important," *The Economist*, October 26, 2015, http://www.economist.com/blogs/economist-explains/2015/10/economist-explains-24.
[17] Stephen Perry, "Chairman's Commentary: The foolish old man who moved the mountain – China thinks in decades and centuries," *The 48 Group Club*, Accessed February 20, 2016, http://the48groupclub.com/2015/06/the-foolish-old-man-who-moved-the-mountain-china-thinks-in-decades-and-centuries-edit/.
[18] Kallie Szczepanski, "People's Republic of China – Facts and History," *About.com Asian History*, December 16, 2014, http://asianhistory.about.com/od/china/p/ChinaProfile.htm.

policy toward China for the past four decades, he had long been one of many in the federal government pushing the US toward full cooperation with China, including heavy financial and technological support, under the belief that the country was headed in a more democratic, free-market direction.

"Looking back, it was painful that I was so gullible," he writes.

Pillsbury notes that he and many other China experts were taught early on to view China as "a helpless victim of Western imperialists" and that as such, assistance should be provided almost unquestioningly.

Now, he says, he has come to consider this view — which he now believes came about as a result of intentional deception and misdirection on the part of the Chinese — as "the most systemic, significant and dangerous intelligence failure in American history."

"We believed that American aid to a fragile China whose leaders thought like us would help China become a democratic and peaceful power without ambitions of . . . global dominance," he writes.

"We underestimated the influence of China's hawks. Every one of the assumptions behind that belief was wrong — dangerously so."

"For decades," Pillsbury adds, "the US government has freely handed over sensitive information, technology, military know-how, intelligence and expert advice to the Chinese. Indeed, so much has been provided for so long that . . . there is no full accounting. And what we haven't given the Chinese, they've stolen."[19]

There can be no doubt that the Total War strategy is being implemented. Its goal is "to use all means whatsoever—to force the enemy to serve one's own interests."[20] As just one small example, Unrestricted Warfare advocates hacking critical systems and declares that new-concept weapons include exposing "the leaders

[19] Larry Getlen, "China's secret plan to topple the US as the world's superpower," *NY Post*, February 8, 2015, http://nypost.com/2015/02/08/chinas-secret-plan-to-topple-the-us-as-the-worlds-superpower/.
[20] Qiao and Santoli, *Unrestricted Warfare*, 43.

of an enemy country on the Internet" through a computer virus invasion.[21] Could there be a more apt description of the likely motive behind the audacious hack of Washington's Office of Personnel Management (OPM)?[22] Even the response to getting caught is straight from the UW playbook, denying any government involvement and blaming criminal activity while maintaining access to the stolen information.[23]

The ultimate goal is to displace the United States as the world's sole superpower. Both the process and the outcome of the endgame are particularly ominous as explained in the text:

> …if the attacking side secretly musters large amounts of capital … launches a sneak attack against financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment … while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis.[24]

We have more than sufficient evidence to conclude that China is active or developing capabilities in each area as described. The only rational conclusion is that China is planning on global dominance.

A few courageous groups such as the Center for Security Policy and the NSIC Institute do have active efforts to bring awareness to this significant threat. The approach is to integrate thinking across disciplines (as required to respond to a true Total War strategy) and to illuminate responses and applications for policy makers,

---

[21] Qiao and Santoli, *Unrestricted Warfare,* 14.

[22] Shane Harris, "Team Obama Knows China Is Behind the OPM Hack. Why Won't They Say So?" *The Daily Beast,* July 20, 2015, http://www.thedailybeast.com/articles/2015/07/20/team-obama-knows-china-is-behind-the-opm-hack-why-won-t-they-say-so.html.

[23] Bill Gertz, "China Says OPM Hack Was Not State-Sponsored," *Washington Free Beacon*, December 2, 2015, http://freebeacon.com/national-security/china-says-opm-hack-was-not-state-sponsored.

[24] Qiao and Santoli, *Unrestricted Warfare,* 123.

the defense and intelligence establishment, investors, and the general public. This chapter represents another step forward in that important work.

Given the virtually limitless nature of the topic of Unrestricted Warfare, it becomes necessary to narrow the focus to a few critical examples. For this purpose, this chapter provides a brief overview of Chinese cyber-economic warfare as it relates to stock market attacks, Intellectual Property (IP) theft, and currency warfare.

The Stock Market Crash Weapon

One of the most striking challenges of Unrestricted Warfare is the reality that a single, man-made stock market crash is a new concept weapon. Before delving into whether this might even be possible, it is necessary to determine the potential impact. Could a stock market crash prove devastating? The answer is an unequivocal "Yes."

The 2008 market crash directly cost investors over $5 trillion in their holdings of the largest 500 public companies (as measured by the S&P 500) during 2008.[25] The overall global economic impact was far greater, however, an estimated 10 times larger at $50 trillion.[26] At the end of 2015, the market value of the S&P 500 was over $18 trillion. A typical market crash could wipe off 40% of market values or more. The direct losses would be over $7 trillion and the global impact might be close to $70 trillion. These are staggering figures as the estimated cost of the Iraq war was about $2 trillion.[27] Of course, a well-executed stock market attack might result in far greater losses. The 2008 crash was ultimately managed through aggressive fiscal spending and unprecedented Central Bank response, neither of which remains available today.[28] According to every major policymaker, the system was staring into

[25] "S&P 500 Index – Historical Total Market Cap," *Market Capitalizations website,* Accessed February 20, 2016, http://marketcapitalizations.com/historical-data/total-market-cap-sp-500/.
[26] "Global Financial Market Losses Reach $50 Trillion, Says Study," *Asian Development Bank*, March 9, 2009, http://www.adb.org/news/global-financial-market-losses-reach-50-trillion-says-study.
[27] Daniel Trotta, "Iraq war costs U.S. more than $2 trillion: study," *Reuters,* March 14, 2013, http://www.reuters.com/article/us-iraq-war-anniversary-idUSBRE92D0PG20130314.
[28] Patrick Gillespie, "Global central banks are running 'out of ammo'," *CNN Money*, February 9, 2016, http://money.cnn.com/2016/02/09/news/economy/global-central-banks-options/.

the abyss.[29] Representative Paul Kanjorski (then Chairman of the House Capital Markets Subcommittee) noted in a C-SPAN interview that there may have been an attack in 2008 and that disaster was narrowly averted:

> On Thursday (Sept 18, 2008), at 11am the Federal Reserve noticed a tremendous draw-down of money market accounts in the U.S., to the tune of $550 billion was being drawn out in the matter of an hour or two. The Treasury opened up its window to help and pumped a $105 billion in the system and quickly realized that they could not stem the tide. We were having an electronic run on the banks. They decided to close the operation, close down the money accounts and announce a guarantee of $250,000 per account so there wouldn't be further panic out there.
>
> If they had not done that, their estimation is that by 2pm that afternoon, $5.5 trillion would have been drawn out of the money market system of the U.S., would have collapsed the entire economy of the U.S., and within 24 hours the world economy would have collapsed. It would have been the end of our economic system and our political system, as we know it.[30]

Notice how closely this description mirrors the UW endgame strategy described earlier with phrases beginning with "launch a sneak attack against financial markets," and ending with "cause the enemy nation to fall into social panic, street riots, and a political crisis."[31] Certainly ending our "economic system and our political system as we know it" qualifies as devastating and aligns with the desired outcome of Total War. The question then becomes whether or not a foreign nation or terror group would have the capacity to cause such an outcome. Frighteningly, the answer to this question is also an unequivocal "yes."

---

[29] Nick Mathiason, "Three weeks that changed the world," *The Guardian*, December 27, 2008, http://www.theguardian.com/business/2008/dec/28/markets-credit-crunch-banking-2008.
[30] Tyler Durden, "How The World Almost Came To An End At 2PM On September 18," *Zero Hedge*, February 8, 2009. http://zerohedge.blogspot.com/2009/02/how-world-almost-came-to-end-at-2pm-on.html.
[31] Qiao and Santoli, *Unrestricted Warfare,* 123.

We know that there was economic warfare involved in the 2008 crash. Former Treasury Secretary Hank Paulson admitted this in a 2014 BBC interview.[32] Ironically, in that case, Russia was leading the attack and China apparently chose not to cooperate but instead informed Paulson.[33] I personally did extensive research for a unit within the Department of Defense regarding the role economic warfare may have played as a trigger of the 2008 crash.[34] These findings were reported in a 2012 book with the title *Secret Weapon: How Economic Terrorism Took Down the U.S. Stock Market and Why It Could Happen Again.*[35] There is little doubt that the Unrestricted Warfare strategy was in play at this time, even if not by the Chinese.

At times almost grudgingly, the defense and intelligence community has acknowledged the reality that a foreign national has the capacity to severely impact, if not outright destroy our financial markets and economy. Former NSA head, General Keith Alexander admitted as much in a 60 Minutes interview:

> On the CBS 60 Minutes tonight, National Security Agency (NSA) director Gen. Keith Alexander admitted that "a foreign national could impact and destroy a major portion of our financial system" by placing a virus in our computer systems "and literally take down the U.S. economy" if the virus was spread around. Alexander told CBS in blunt terms that "right now it would be difficult to stop (the virus attack) because our ability to see it is limited."[36]

---

[32] Robert Peston, "Russia 'planned Wall Street bear raid'," *BBC News*, March 17, 2014, http://www.bbc.com/news/business-26609548.

[33] Tyler Durden, "Russia Urged China To Dump Its Fannie, Freddie Holdings Before GSE Bailout," *Zero Hedge,* January 29, 2010, http://www.zerohedge.com/article/russia-urged-china-dump-its-fannie-freddie-holdings-gse-bailout.

[34] Bill Gertz, "Financial terrorism suspected in 2008 economic crash," *The Washington Times,* February 28, 2011, http://www.washingtontimes.com/news/2011/feb/28/financial-terrorism-suspected-in-08-economic-crash/?page=all.

[35] Kevin Freeman, *Secret Weapon: How Economic Terrorism Brought Down the U.S. Stock Market and Why It can Happen Again,* (Washington, DC: Regnery Publishing, Inc., 2012).

[36] Robert Lenzner, "Some Foreign Nations Have the Cyberwar Capability to Destroy Our Financial System, NSA Admits," *Forbes,* December 15, 2013, http://www.forbes.com/sites/robertlenzner/2013/12/15/some-foreign-nations-have-cyberwar-capability-to-destroy-our-financial-system-nsa-admits/#392f431b5b813.

General Alexander's testimony merely echoes what is whispered but largely ignored behind closed doors in DC., especially following the mysterious "flash crash" of 2010.[37] Consider this from BARRON'S in 2011:

> But witnesses before an informal convocation of the House Committee on Homeland Security on July 20 were united in their conviction that the nation's 10 or so stock exchanges and 50-plus related trading venues are vulnerable to attacks from traders overseas . . . Foreigners theoretically could gain "naked access" to an exchange through the sponsorship of a brokerage firm. This means that the broker would allow a paying customer to co-locate its own servers with the broker's servers in a facility with a direct, high-speed connection to the exchange's servers. This proximity reduces trading "latency." In other words, the shorter the connection, the faster the round trip from trader to exchange.[38]

Despite this reality, it appears that a Chinese company may be allowed to buy the Chicago Stock Exchange providing exactly the kind vulnerability warned against:

> While one of the oldest in the US at 134 years, the Chicago exchange is also a measly one in the grand scheme of things--the third smallest in the country, to be specific. Valued at under $100 million, the exchange handles about 0.5% of America's stock trading. But it gets Chongqing Casin a foot in the door of the competitive $22 trillion US equity market, with hope for future growth. [39]

The deal actually leapfrogs brokerage firm access by granting exchange-level status to a Chinese corporation.

---

[37] Francine McKenna, "SEC's panel still at a loss over how to fix 'broken market'," *Market Watch*, June 30, 2015, http://www.marketwatch.com/story/five-years-after-flash-crash-committee-to-fix-markets-can-barely-agree-an-agenda-2015-06-30.

[38] Jim McTague, "How Foreigners Could Disrupt U.S. Markets," *University of Delaware Library*, September 11, 2010, http://green.lib.udel.edu/webarchives/kaufman.senate.gov/press/in_the_news/news/-id=0a760c05-5056-9502-5df6-cc9220d44e1d.htm.

[39] "Chinese company buys Chicago Stock Exchange," *Shanghiist*, February 8, 2016, http://shanghaiist.com/2016/02/08/chinese_company_buys_chicago_stock.php.

We know that larger exchanges are vulnerable to hacking as it was reported that Russians placed a "digital bomb" inside the NASDAQ in 2010.[40] We also know that cyber capabilities are not limited to larger nations. The Syrian Electronic Army reportedly caused a $136 billion stock market drop by hacking the Associated Press Twitter feed, triggering program selling by High-Frequency Traders.[41] According to billionaire investor Mark Cuban, High-Frequency Traders create an entirely new level of vulnerability.[42]

Even if the intentions of High-Frequency Traders were honorable, the fact that computer algorithms have unrestrained capability to move markets highlights the hacking vulnerability. What if the trading algorithms were compromised as Goldman Sachs alleged happened to them?[43] Before regulators might realize, a compromised firm could easily trigger a massive market meltdown that might take years to unsort. Combined with other attacks outlined in the UW strategy, such as taking down the civilian electricity network, the end result could be total collapse.

> While China has been discreet regarding their market crash capabilities, Russia has been more direct:
>
> Russia … could cause the Dow Jones industrial average to plummet, as it has never done before. One can wave the Stars and Stripes as long as one likes, but it's a fact that the Russians can turn the US economy upside down, Sinclair warns.[44]

---

[40] Jose Pagliery, "Russian hackers placed 'digital bomb' in Nasdaq – report," *CNN Money,* July 17, 2014, http://money.cnn.com/2014/07/17/technology/security/nasdaq-hack/.

[41] Max Fisher, "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?" *The Washington Post,* April 23, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

[42] Kevin Freeman, "'Knightmare' on Wall Street," *Global Economic Warfare website,* August 3, 2012, http://globaleconomicwarfare.com/2012/08/knightmare-on-wall-street/.

[43] Kim Zetter, "Programmer convicted in bizarre Goldman Sachs case – again," *Wired,* May 1, 2015, http://www.wired.com/2015/05/programmer-convicted-bizarre-goldman-sachs-caseagain/.

[44] Igor Siletsky, "Russia's secret weapon: crashing US economy by collapsing petrodollar," *Sputnik News*, March 28, 2014, http://sputniknews.com/voiceofrussia/news/2014_03_28/Russia-s-secret-weapon-crashing-US-economy-by-collapsing-petrodollar-5071/.

We also know that the FBI arrested an alleged Russian spy who they said was seeking ways to destabilize stock markets using Exchange-Traded Funds.[45] If Russia has sought and obtained the capability to cause a stock market crash, it is most certainly true that the Chinese have this capability as well. If, as the U.S. government has alleged, a small-time trader in London could trigger the "flash crash," what could a powerful nation do?[46]

Ironically, the Chinese have accused America of attempting to crash their stock market as an act of economic warfare.[47] This suggests two things. First, they understand the reality of the weapon. Second, they have established justification for retaliation.

Obviously, it is not in China's interest to take down America if that would irreparably harm China's future as well. Certainly that has been the case and likely remains so today. However, it is important to note that China, along with Russia and a few others, has been feverishly establishing an integrated alternative to the Western financial system.[48] When that process is completed, the blowback damage potential will be sharply reduced. The Chinese "single manmade stock market crash" weapon will be a full-blown reality.

Intellectual Property (IP) Theft

Beyond the "kill shot" of a stock market crash, the Chinese have also adopted UW techniques to undermine American technology development and enrich themselves via IP theft.[49] The goal is "to use all means whatsoever—to force the enemy to serve one's own interests."[50]

---

[45] Siletsky, "Russia's secret weapon."

[46] Nathaniel Popper and Jenny Anderson, "Trader Arrested in Manipulation That Contributed to 2010 'Flash Crash'," *The New York Times,* April 21, 2015, http://www.nytimes.com/2015/04/22/business/dealbook/trader-in-britain-arrested-on-charges-of-manipulation-that-led-to-2010-flash-crash.html?_r=0.

[47] Miles Yu, "Official: China stock crash is U.S. economic warfare," *The Washington Times,* July 23, 2015, http://www.washingtontimes.com/news/2015/jul/23/inside-china-official-china-stock-crash-is-us-econ/?page=all.

[48] Jeff Thomas, "Schadenfreude – How The US Is Helping China Create A New Financial Order," *Zero Hedge website,* October 26, 2015, http://www.zerohedge.com/news/2015-10-26/schadenfreude-how-us-helping-china-create-new-financial-order.

[49] Paulo Shakarian, Jana Shakarian, and Andrew Ruef, "The Dragon and the Computer: Why Intellectual Property Theft is Compatible with Chinese Cyber-Warfare Doctrine," from:

While IP theft can be more akin to bleeding an economy rather than killing it, the cost is still enormous, estimated by one report to be around $300 billion annually with up to 80% directly tied to China.[51] Adding in the technology transfer that displaces legitimate business and the losses could be as high as $5 trillion per year, or up to 30% of our economy according to an Epoch Times report:

> 'Our intelligence unit's latest estimates are that U.S. companies and the U.S. economy lose approximately $5 trillion each year, or over 30 percent of the U.S. GDP when you factor the full value of the stolen innovation,' Fleming said.
>
> 'It will not take long for every American citizen to be affected by the scale of this economic espionage assault in the form of lost jobs, higher prices, and a lower quality of life,' he said.[52]

Granted, the gap between an estimated $300 billion per year in IP losses and $5 trillion per year is large. To explain this, Epoch Times identifies how the IP stolen and then reverse engineered to dramatically undercut American technology and manufacturing in global markets:

Elements of China's military, state, business, and academia have been interwoven over decades and organized around one goal: stealing secrets from the West. This regime of theft takes with impunity, powering China's economy and high-tech military, while robbing the United States alone of trillions in value each year.

Very late in the game, the United States has started to respond. The U.S. Justice Department made headlines in May 2014 by indicting five Chinese military hackers from Unit 61398 for their alleged role in economic theft.

Introduction to Cyber-Warfare: A Multidisciplinary Approach, (Waltham, MA: Elsevier, Inc., 2013), http://arxiv.org/pdf/1309.6450.pdf.

[50] Qiao and Santoli, *Unrestricted Warfare,* 43.

[51] "US report warns on China's massive intellectual property theft," *The Economic Times,* May 23, 2013, http://articles.economictimes.indiatimes.com/2013-05-23/news/39475776_1_ip-theft-china-foreign-ip.

[52] Joshua Philipp, "EXCLUSIVE: How Hacking and Espionage Fuel Chain's Growth," *The Epoch Times,* September 10, 2015, http://www.theepochtimes.com/n3/1737917-investigative-report-china-theft-incorporated/.

The system, however, doesn't stop at military hackers. Organizations throughout China work as "transfer centers" that process stolen information into usable designs. Official programs facilitate the theft. And the whole system runs through a corrupt nexus among government officials, military officers, business executives, and academics throughout China.[53]

In other words, this is a "Total War" strategy for China and it is robbing America blind:

> There are an estimated 3,000+ front companies operated by the PLA in the US which exist solely to steal American tech, the report alleged, quoting official government sources.[54]

The impact extends beyond economic loss, however, as the loss of innovation is directly impacting our military capabilities. The first realization is that IP theft undermines innovation:

> The second and even more pernicious effect is that illegal theft of IP is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries…[55]

Now, couple that reality with the fact that the defense industry is losing its technological edge as noted in a report in The Wall Street Journal:

> …Defense Secretary Ash Carter faces two challenges. The first is getting Americans and their elected representatives to recognize the technological stagnation.
>
> Today almost none of the new military equipment coming online is revolutionary in design or technology; most is merely an upgraded version of something from the Cold War. A half-century ago, the Pentagon had more than a dozen combat aircraft in development. Last year it had only the late and over budget F-35 and a new bomber. The

[53] Philipp, "How Hacking."
[54] Phil Muncaster, "China's IP Theft and Tech Transfer Network Costs US $5 Trillion – Report," *Info Security Magazine website,* September 15, 2015, http://www.infosecurity-magazine.com/news/chinas-ip-theft-tech-transfer/.
[55] "US report warns."

American public believes its military is No. 1, but its commanders and its enemies increasingly know differently.

The Pentagon has fallen behind the pace of commercial innovation … America's challengers abroad, meanwhile, are catching up and surpassing us. China's air-to-air missiles outrange those of the U.S. Air Force, and Beijing continues to invest in developing hypersonic missiles, which travel so fast that defending against them would be almost impossible. Russia has taken the lead in electronic warfare, even as the U.S. continues to rely on Russian rocket engines to launch satellites and the Soyuz capsule to transport American astronauts to the international space station. In August the former commander of the Army's electronic-warfare division said this of the Russians: "We can't shut them down one-tenth to the degree they can us. We are very unprotected from their attacks on our network."

Declining technological superiority is felt even more as the U.S. military continues to shrink and is now 36% smaller than at the end of the Cold War. Falling margins of pre-eminence sow doubt in the ranks; the U.S. military isn't accustomed to fighting fair. Combat without a technological advantage will mean mission failures, higher casualty rates and longer wars.

Losing is no longer unthinkable. Beginning in 2014, former Pentagon force planner David Ochmanek ran war games examining whether the U.S. and NATO could defend the Baltics against an attempted Russian takeover. He ran 16 war games with eight different teams of military personnel; the U.S. lost every time. The exercise disproved the assumption that America's supposed technological edge would make up for U.S. forces' being outnumbered in Europe.

Although these facts weigh on military leaders, they are received coolly by Congress. Many lawmakers deny that a problem exists, or think that these claims are made up to justify a bigger military budget.

Secretary Carter's second challenge is to repair the cultural and regulatory divides between the Pentagon and tech companies. The truth is that the military cannot easily tap into private-industry innovation. Washington's

> debates over forcing tech companies to open back doors into encrypted communications systems, along with the leaks about NSA surveillance by Edward Snowden, have fomented enormous distrust. Skilled entrepreneurs and engineers are not interested in working for the government. Worse, structural problems in the Pentagon's acquisition system deter nontraditional contractors from doing business with the military.[56]

Essentially, this means that while the American military has been stifled in innovation, the Chinese PLA has been able to steal the latest technology. This could not be clearer than in the case of the F-35:

> China obtained more than 50 terabytes of data from U.S. defense and government networks, notably the Joint Strike Fighter's stealth radar and engine secrets, through cyber espionage, according to newly disclosed National Security Agency documents.
>
> A NSA briefing slide labeled "Top Secret" and headlined "Chinese Exfiltrate Sensitive Military Data," states that the Chinese have stolen a massive amount of data from U.S. government and private contractors. [The NSA briefing slide was posted at Spiegel: http://www.spiegel.de/media/media-35687.pdf]
>
> The document was made public by the German magazine Der Spiegel in a two articles detailing how NSA in the mid-2000s was capable of conducting global cyber intelligence-gathering by tapping into the networks of foreign intelligence services and stealing the data they were collecting from others….
>
> The NSA also revealed that the Air Force's networks were infiltrated by Chinese hackers, an attack that resulted in the loss of 33,000 records for general and field grade officers.
>
> Navy losses to Chinese hackers included data on missile navigation and tracking system, nuclear submarine and anti-aircraft missile design and over 300,000 user identification and passwords.

[56] Mackenzie Eaglen, "Tech-Challenged Pentagon Searches for a Silicon Ally," *The Wall Street Journal,* January 31, 2016, http://www.wsj.com/articles/tech-challenged-pentagon-searches-for-a-silicon-ally-1454282727.

> The Chinese also obtained sensitive science and technology data controlled for export from U.S. networks, including International Traffic and Arms Restrictions (ITAR) secrets, and contractor research and development.
>
> In all, the NSA concluded that the Chinese compromised key weapons systems including the F-35, the B-2 bomber, the F-22 fighter-bomber, the Space Based Laser, and other systems.
>
> The amount of stolen data was "the equivalent of five Libraries of Congress (50 terabytes)," the NSA said. A terabyte is 1,000 gigabytes. [57]

There should be little doubt that IP theft is a critical part of China's Unrestricted Warfare approach.

Currency Warfare

Chinese currency manipulation is a third threat to America's future. Rather than allowing a true floating currency, the Chinese government has carefully controlled the exchange rate to suit its purposes. When beneficial, China has been prepared to devalue and gain global market share.[58] And, when it would prove advantageous, China is prepared to strengthen the yuan and displace the American dollar entirely.[59]

This is entirely consistent with the UW strategy as the Chinese book explained:

> Instead, it must adjust its own financial strategy, use currency revaluation or devaluation as primary, and combine means such as getting the upper hand in public opinion and changing the rules sufficiently to make

[57] Bill Gertz, "NSA Details Chinese Cyber Theft of F-35, Military Secrets," *Washington Free Beacon,* January 22, 2015, http://freebeacon.com/national-security/nsa-details-chinese-cyber-theft-of-f-35-military-secrets/.
[58] Former Representative Bill Owens, "Time to take action against Chinese currency manipulation," *The Hill,* August 20, 2015, http://thehill.com/blogs/pundits-blog/finance/251534-time-to-take-action-against-chinese-currency-manipulation.
[59] Dimitra DeFotis, "China: Yuan Will Replace U.S. Dollar?" *Barron's,* November 16, 2015, http://blogs.barrons.com/emergingmarketsdaily/2015/11/16/china-why-the-yuan-will-replace-the-u-s-dollar/.

> financial turbulence and economic crisis appear in the targeted country or area, weakening its overall power, including its military strength.[60]

At times, China has used the exchange-rate mechanism to lower the yuan valuation in global markets, as was the case in August 2015:

> China's currency last week dropped by a cumulative 4.4% against the U.S. dollar, making Chinese exports cheaper and imports into China more expensive by that amount.
>
> The effect on trade can be substantial. With the U.S. average tariff on industrial goods well under 2%, this change in China's currency value easily swamps most U.S. tariffs. And given the fact that the U.S. dollar was already strong, this move is an added disadvantage to U.S. exports headed for China compared to exports from other countries.
>
> As world leaders continue negotiating what's poised to be a landmark trade deal across the Pacific Rim, some U.S. lawmakers have responded with criticism: "Today's provocative act by the Chinese government to lower the value of the yuan is just the latest in a long history of cheating," said Republican U.S. Sen. Lindsey Graham…[61]

The impact on global economies can be dramatic as explained:

> The effects on world trade due to government intervention into the foreign exchange market can be dramatic. As a result of the Chinese government's intervention into RMB's foreign exchange rate in an effort to control its appreciation, Chinese goods are exported at a cheaper rate, requiring less foreign currency to purchase. Conversely, its imports become more expensive, requiring more domestic currency to purchase foreign goods. Economists contend that the undervalued RMB has been a major factor in the fast-growing U.S. trade deficit with China, which has skyrocketed from $10 billion in 1990 to $273 billion in 2010.[62]

---

[60] Qiao and Santoli, *Unrestricted Warfare,* 167.

[61] Alan Wolff, "What China's currency devaluation means for the world's trade deals," *Fortune,* August 19, 2015, http://fortune.com/2015/08/19/what-chinas-currency-devaluation-means-for-the-worlds-trade-deals/.

[62] Anthony Yu, "China's Currency Practices and 'Currency Manipulation': The Power of Action in Inaction," *McGeorge*, 22 July, 2013, http://www.mcgeorge.edu/Documents/Publications/262_7Yu.pdf.

The U.S.- China trade deficit has continued to grow and now measures over $365 billion annually.[63] But the impacts don't end with the trade deficit. The Federal Reserve was tasked with reviewing a Chinese devaluation of up to 15% and suggested that such a move would "reduce U.S. GDP by 0.48 percent ($99 billion), increasing the trade deficit by $66 billion … eliminating 640,000 U.S. jobs."[64]

This would seem to be another strategy to bleed America. Unfortunately, currency manipulations can provide a "kill shot" as well. A former KGB Putin advisor explained as early as 1998 how a U.S. debt failure and a dollar collapse could trigger the demise of the United States, (as reported in The Wall Street Journal:

> Prof. Panarin, 50 years old, is not a fringe figure. A former KGB analyst, he is dean of the Russian Foreign Ministry's academy for future diplomats. He is invited to Kremlin receptions, lectures students, publishes books, and appears in the media as an expert on U.S.-Russia relations…
>
> But it's his bleak forecast for the U.S. that is music to the ears of the Kremlin, which in recent years has blamed Washington for everything from instability in the Middle East to the global financial crisis. In September 1998, he attended a conference in Linz, Austria, devoted to information warfare, the use of data to get an edge over a rival. It was there, in front of 400 fellow delegates, that he first presented his theory about the collapse of the U.S.
>
> Mr. Panarin posits, in brief, that mass immigration, economic decline, and moral degradation will trigger a civil war…and the collapse of the dollar … (he) called U.S. foreign debt "a pyramid scheme," and predicted

[63] Terence P. Jeffrey, "$365,594,500,000: U.S. Merchandise Trade Deficit With China Hit Record in 2015," *CNS News,* February 9, 2016, http://cnsnews.com/news/article/terence-p-jeffrey/365694500000-merchandise-trade-deficit-china-hit-record-2015.

[64] Robert E. Scott, "Congress Must Act to Save the 190,000 to 640,000 U.S. Jobs a Risk Due to Chinese Currency Devaluation," *Economic Policy Institute,* August 17, 2015, http://www.epi.org/blog/congress-must-act-on-chinese-currency-devaluation/.

> China and Russia would usurp Washington's role as a global financial regulator.[65]

It is significant to note that Panarin expected the U.S. to collapse around the year 2010 and that obviously did not happen. But, as noted earlier, the Russian government did attempt an economic attack in 2008, even soliciting Chinese support at the time.[66] The Chinese rejected the plan and may have started to regret it as early as 2010 as explained in an article that appeared in Quishi, the official publication of the Central Committee of the Communist Party of China. This article explained how China could counter the United States using economic weapons. Note the emphasis on the need for courage and determination to confront the United States:

> Economic Warfare. Of course, to fight the U.S., we have to come up with key "weapons." What is the most powerful weapon China has today? It is our economic power, especially our foreign exchange reserves. The key is to use it well. If we use it well, it is a weapon; otherwise it may become a burden. Counting on the fact that the U.S. dollar is the international currency, the U.S. government has increased the number of dollars in circulation, leading to its devaluation. The countries with high reserves in dollars will suffer, but the U.S. itself loses nothing. However, for this to be true there is a premise. Someone must purchase those excess dollars they printed. If no one purchases them, then they will only be circulated domestically, inside the U.S., and cause inflation. In order for the countries with foreign exchange reserves in the U.S. dollar to restrain the U.S. from over-issuing U.S. currency, they must act together and not buy U.S. dollars … The key to success is that China needs to have enough courage and determination to take the U.S. pressure. This is exactly what we need. It just shows how much the U.S. needs China. The more pressure we can take, the more successful this strategy. It will indicate that this "weapon" is highly effective and the U.S. will start to fear us.

---

[65] Andrew Osborn, "As if Things Weren't Bad Enough, Russian Professor Predicts End of U.S." *The Wall Street Journal,* December 29, 2008, http://www.wsj.com/articles/SB123051100709638419.

[66] Durden, "Russia Urged China."

> Financial War. The fact that the U.S. dollar is the world's reserve currency makes the U.S. a financial superpower. Currently, China's increased share in the International Monetary Fund and its increased voting rights are a very big step forward. The problem is not that the value of this share is expressed in U.S. dollars, but that it would be best if the share could be expressed in RMB. Therefore, for China to challenge the position of the U.S. dollar, it needs to take a path of internationalization and directly confront the U.S. dollar… We fully trust the Chinese government's capacity to handle the market and the regulations. If these four suggested actions can be implemented smoothly using the market mechanism, the RMB will become the world's reserve currency, putting pressure on the U.S. dollar and undermining U.S. financial strength.[67]

The official Chinese position went further in 2013 with a call to officially "de-Americanize the world," and to remove the dollar as the world's reserve currency.[68] Since 2013, China has made substantive moves, often with Russia to establish an entirely non-American financial framework.[69] In addition, the nation has jockeyed into a position where the IMF will count the Chinese yuan as a global reserve currency.[70]

The idea of a Chinese-led currency regime replacing the dollar was considered nearly impossible not long ago.[71] The official American position has been articulated that the dollar is a permanent global reserve currency no matter what the

---

[67] TL, LD, AF, and AT, trans. "How China Deals with the U.S. Strategy to Contain China," *China Scope*, December 10, 2010, http://chinascope.org/main/content/view/3291/92/.

[68] Liu Chang, "Commentary: U.S. fiscal failure warrants a de-Americanize world," *Xinhua News,* October 13, 2013, http://news.xinhuanet.com/english/indepth/2013-10/13/c_132794246.htm.

[69] Lawrence H. Summers, "Time US leadership woke up to new economic era," *Larry Summers website,* April 5, 2015, http://larrysummers.com/2015/04/05/time-us-leadership-woke-up-to-new-economic-era/.

[70] Ian Talley, "China Joins World's Elite Currency Club," *The Wall Street Journal*, November 30, 2015, http://www.wsj.com/articles/imf-lifts-chinese-yuan-to-elite-lending-reserve-currency-status-1448903067.

[71] Via WikiLeaks, "London-based Experts agree the U.S. dollar will maintain its reserve status," *The Telegraph,* February 4, 2011, http://www.telegraph.co.uk/news/wikileaks-files/london-wikileaks/8305279/LONDON-BASED-EXPERTS-AGREE-THE-U.S.-DOLLAR-WILL-MAINTAIN-ITS-RESERVE-STATUS.html.

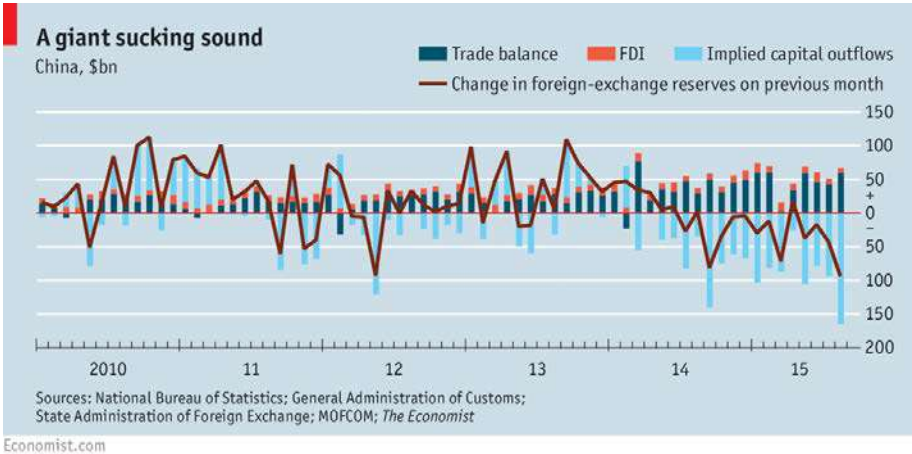
Chinese do.[72] Treasury Secretary Timothy Geithner shared this thought when visiting China a few years ago. He was laughed out of the room as the Chinese firmly expect the U.S. dollar to fail.[73]

More recently, Secretary of State Kerry admitted that the idea of a failed dollar was "bubbling out there" and that there are conditions under which the dollar could lose its reserve currency status.[74] The Chinese sense American weakness with our Federal debt over $19 trillion (roughly double the level of 2008).[75] They also are aware that the Federal government has over $200 trillion in unfunded liabilities.[76] Thus, academics have recommended a drawdown of dollar assets.[77] The PLA has also urged that U.S. debt be exploited as a weapon.[78]

Of course, the Chinese have plenty of their own domestic economic problems. Yes, they still have more than $3.2 trillion in official foreign currency reserves (down from close to $4 trillion).[79] Yes they have an undisclosed pile of gold covertly acquired in recent years.[80] And, it is widely believed that the Chinese have

[72] Jon Nielsen, "No risk to dollar if China expands yuan's role: Geithner," *Reuters,* March 8, 2012, http://www.reuters.com/article/us-usa-taxes-idUSBRE8271AZ20120308.
[73] Joe Weisenthal, "Chinese Students Laugh At Tim Geithner," *Business Insider,* June 1, 2009, http://www.businessinsider.com/chinese-students-laugh-at-tim-geithner-2009-6.
[74] Sharona Schwartz, "John Kerry Warns of Dire Consequence for the Dollar if Congress Rejects Iran Deal," *The Blaze,* August 12, 2015, http://www.theblaze.com/stories/2015/08/12/john-kerry-warns-of-dire-consequence-for-the-dollar-if-congress-rejects-iran-deal/.
[75] US Debt Clock, http://www.usdebtclock.org.
[76] Barbara Hollingsworth, "Economist Tells Congress: U.S. May Be in 'Worse Fiscal Shape' Than Greece," *CNS News*, March 9, 2015, http://www.cnsnews.com/news/article/barbara-hollingsworth/economist-tells-congress-us-may-be-worse-fiscal-shape-greece.
[77] David Li, "Beijing should cut back its lending to Washington," *Financial Times,* October 15, 2013, http://www.ft.com/intl/cms/s/0/2d7f44ec-3585-11e3-b539-00144feab7de.html?siteedition=intl#axzz2htGddpzm.
[78] Joe Chan, "China PLA officers urge economic punch against U.S." *Reuters,* February 9, 2010, http://www.reuters.com/article/us-china-usa-pla-idUSTRE6183KG20100209.
[79] Jethro Mullen and Sophia Yan, "China's foreign currency stockpile fell nearly $100 billion last month," *CNN Money,* February 7, 2016, http://money.cnn.com/2016/02/07/news/economy/china-foreign-currency-reserves-january/.
[80] Tyler Durden, "Chart Of The Day: China Imports Over 2,000 Tons Of Gold In Last Two Years," *Zero Hedge website,* October 13, 2013, http://www.zerohedge.com/news/2013-10-13/chart-day-china-imports-over-2000-tons-gold-last-two-years.

bought influence around the world.[81] But their domestic bad loans are substantial.[82] Some believe the regime is under serious threat and may not survive.[83] This is being evidenced in a serious capital flight that has taken place recently.[84]



This creates the concern that a wounded dragon may be the most dangerous type. Domestic weakness may force the Chinese to act sooner than planned with an emphasis on military power.[85] For example, China has already started reducing its holdings of American debt. At the same time, China has ramped up military spending.[86]

It is possible that the ruling Party will act in desperation, believing that if the dollar were displaced, global reserves would flock to China providing capital essential

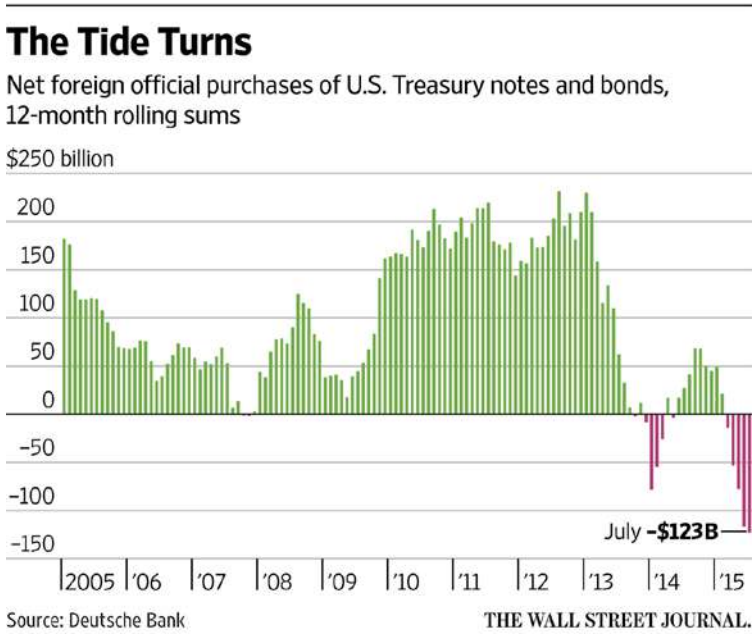
[81] Scott L Kastner, "Buying Influence? Assessing the Political Effects of China's International Trade," Journal of Conflict Resolution (2014): 0022002714560345, http://jcr.sagepub.com/content/early/2014/12/26/0022002714560345.abstract.
[82] Michael Pettis, "Bad loans could take their toll on China's growth," *Financial Times,* August 21, 2010, http://www.ft.com/intl/cms/s/0/9d2a0448-4d77-11df-9560-00144feab49a.html#axzz3zimRHDBG.
[83] Ho-Fung Hung, Arthur R. Kroeber, Howard W. French, and Suisheng Zhao, "When Will China's Government Collapse?" *Foreign Policy,* March 13, 2015, http://foreignpolicy.com/2015/03/13/china_communist_party_collapse_downfall/.
[84] "Capital flight is at the core of China's dilemma," *Financial Times,* January 13, 2016, http://www.ft.com/intl/cms/s/0/b5d26b4c-b9f1-11e5-b151-8e15c9a029fb.html#axzz3zimRHDBG.
[85] Alexander Sullivan and Andrew S. Erickson, "The Big Story Behind China's New Military Strategy," *The Diplomat,* June 5, 2015, http://thediplomat.com/2015/06/the-big-story-behind-chinas-new-military-strategy/.
[86] "China military budget 'to rise 10%'," *BBC News,* March 4, 2015, http://www.bbc.com/news/world-asia-china-31706989.

for survival.[87] However unlikely this may seem, even a meager possibility of success might be sufficient to trigger the effort. History is full of examples where desperate international actors ignored long odds with rash actions.

Another concern is that the Chinese may believe that the war has already started with the United States as the aggressor. The Unrestricted Warfare authors viewed George Soros as an agent of the United States and considered him an American financial terrorist.[88] Couple that realization with China's recent warning to Soros to "not go to war" against their currency:

> China's official newspaper warned billionaire investor George Soros not to bet against the Yuan in a front-page opinion piece, as China tries to boost confidence in its home currency, also known as the renminbi, which has dropped 5 percent since August.
>
> "Soros's war on the renminbi and the Hong Kong dollar cannot possibly succeed – about this there can be no doubt," said the article titled "Declaring war on China's currency? Ha ha," published by People's Daily, the official newspaper of the Chinese Communist Party. [89]

[87] Heather Timmons, "Losing the Plot: As China's economy unravels, Beijing's attempts at damage control are growing increasingly desperate," *Quartz,* February 4, 2016, http://qz.com/596745/beijing-controls-the-largest-most-powerful-propaganda-team-on-the-planet-so-why-is-chinas-pr-suddenly-so-awful/.
[88] Qiao and Santoli, *Unrestricted Warfare,* 160.
[89] "China warns George Soros: Don't go to 'war' against our currency," *Russian Times,* January 27, 2016, https://www.rt.com/news/330252-china-warns-soros-currency-war/.



Regardless of whether or not China could succeed in establishing the yuan in global reserve status, it should be clear that a concerted Chinese war on the dollar would do serious damage.[90] If confidence in the dollar failed, our nation would be unable to fund a budget deficit or the debt.[91] This would require serious spending cutbacks including to the military. It is for this reason that terror groups would like to see the dollar fail.[92] It is also why defense experts have stated that our national debt may be our greatest national security threat.[93]

[90] "What if the Yuan competes with the dollar: Clash of the Currencies," *The Economist*, Accessed February 21, 2016, http://worldif.economist.com/article/6/what-if-the-yuan-competes-with-the-dollar-clash-of-the-currencies.
[91] Romina Boccia, "Federal Debt Just Exceeded $19 Trillion: $58,000 for Each Person in U.S." *CNS News,* February 3, 2016, http://www.cnsnews.com/commentary/romina-boccia/us-debt-just-exceeded-19-trillion-equaling-58000-each-person-living-us.
[92] Daveed Gartenstein-Ross, "Bin Laden's 'War of a Thousand Cuts' Will Live On," *The Atlantic,* May 3, 2011, http://www.theatlantic.com/international/archive/2011/05/bin-ladens-war-of-a-thousand-cuts-will-live-on/238228/.
[93] Tim Mak, "Former top military officer sees national debt as biggest threat to country," *The Washington Examiner,* January 21, 2014, http://www.washingtonexaminer.com/former-top-military-officer-sees-national-debt-as-biggest-threat-to-country/article/2542594.

Beyond the sale of Treasury bonds or establishing the yuan as a reserve currency, it has recently surfaced that computer hacking can manipulate exchange rates:

> Hackers used malware to penetrate the defenses of a Russian regional bank and move the ruble-dollar rate more than 15 percent in minutes, according to a Moscow-based cyber-security firm hired to investigate the attack.
>
> Russian-language hackers deployed a virus known as the Corkow Trojan to infect Kazan-based Energobank and place more than $500 million in orders at non-market rates in February 2015, Group-IB told Bloomberg, without identifying individuals behind the attack. The resulting rate swing prompted a Russian central bank investigation into potential market manipulation.
>
> Malicious software of the type used in the attack can open a back door into computers via seemingly legitimate websites or files and then force them to carry out hackers' orders. [94]

Computers now do most currency trading.[95] As a result, the systems are vulnerable to hacking the same as other high-frequency trading platforms.[96] Chinese hackers could literally take control of a firm or exchange and create a dollar collapse that would be largely unexplained but clearly devastating.

The long-standing hope is that China depends too much on the current financial system, based on the U.S. dollar, to undertake any action that might

[94] Jake Rudnitsky and Ilya Khrennikov, "Russian Hackers Moved Ruble Rate With Malware, Group-IB Says," *Bloomberg,* February 8, 2016, http://www.bloomberg.com/news/articles/2016-02-08/russian-hackers-moved-currency-rate-with-malware-group-ib-says.

[95] Lananh Nguyen, "A Dying Breed: Currency Traders Are Left Out of New Wall Street," *Bloomberg,* February 7, 2016, http://www.bloomberg.com/news/articles/2016-02-08/a-dying-breed-currency-traders-are-left-out-of-new-wall-street.

[96] John Detrixhe, Nikolaj Gammeltoft, and Sam Mamudi, "High-Frequency Traders Chase Currencies," *Bloomberg,* April 2, 2014, http://www.bloomberg.com/news/articles/2014-04-02/high-frequency-traders-chase-currencies-as-stock-volume-recedes.

threaten their economy.[97] This is a modern "Mutually Assured Destruction" view. There are three circumstances, however, that would disrupt that balance. First, if China felt that the American position was failing anyway and wanted to have more control in the outcome. Second, if China were desperate and thus forced to take drastic action. Third, if China chose the circumstances and timing as an act of war with an eye toward long-term global dominance. Frighteningly, any of the three is a reasonable possibility.

The bottom line is that China views their currency as a potential weapon and the exchange-rate mechanism as a battle space. The UW strategy has long targeted the dollar and the American economy. There should be little doubt that the Chinese see systemic vulnerability and may be willing to exploit it.

[97] Bill Gertz, "Inside the Ring: New WMD threats," *The Washington Times,* October 10, 2012, http://www.washingtontimes.com/news/2012/oct/10/inside-the-ring-new-wmd-threats/?page=2.

COUNTERING CHINA'S OBJECTIVES IN THE WESTERN PACIFIC

By Admiral James "Ace" Lyons

China's unflinching efforts over the last 20 years to seize control of almost the entire South China Sea is an indication of new assertiveness to advance its regional dominance at the expense of the United States. Since these efforts threaten regional and global security and the international economy, it is crucial that the next president make halting these efforts a top priority.

When the United States withdrew its forces from the Philippines in 1992, a vacuum was created which provided China with an unprecedented opportunity to expand its influence and territorial objectives. In 1993, China announced its illegal claim to almost the entire South China Sea as part of its territorial waters. This claim is based on China's questionable Nine Dash Line Maritime claim and includes large sea areas of internationally recognized economic zones belonging to Vietnam, Brunei, Malaysia, Philippines, Taiwan, and Japan.

It should be noted that while China is a signatory to the United Nations' Law of the Sea Treaty (LOST),[98] it has stated that any sea area it claims as its territorial sea is excluded from arbitration and will not be submitted to any LOST tribunal for resolution. Current claims by the Philippines against China's illegal actions, which have been submitted to the UN LOST tribunal for peaceful resolution, are continually ignored by China.

China's illegal South and East China Sea claims are only part of China's phased expansion of its sea power. China clearly wants hegemony out to the First Island chain, which includes: Taiwan, Okinawa, Rynkyus, and the Philippines. They want to impose military control over this sea area, most likely to protect the PRC's nuclear ballistic submarine operations out of Hainan Island. Furthermore, China wants to ensure that Hainan Island will become a secure base for future power

[98] Treaty Collection, "Chapter XXI: Law of the Sea," *United Nations web site*, Updated February 29, 2016, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXI-6&chapter=21&Temp=mtdsg3&lang=en.

projection operations, aircraft carrier operations, amphibious forces, and meet its need for secure space launch operations.

In the next phase, China wants to expand its hegemony out to the Second Island chain, which includes Guam, a key U.S. Pacific facility. To reinforce its South China Sea claims, China has been on an aggressive reclamation program, creating man-made islands out of shallow reefs and inlets for the past several years. Since 2014, China has reclaimed over 3,000 acres. Construction of airstrips and other permanent facilities have been built on these man-made islands. These islands are, in effect, stationary aircraft carriers.

China has been ignoring President Obama's proposals to take positive steps to lower tensions in the South China Sea, including a halt to further reclamation of new disputed territory. At the First Sea Lord/RUSI International Sea Power Conference[99] on Sept 14, 2015, Chinese Vice Admiral Yuan Yubai stated, "The South China Sea, as the name indicates, is a sea area that belongs to China."[100] For Admiral Yuan, this is the end of the discussion.

China has already taken steps to deploy significant air, naval, and missile forces to its newly reclaimed 14.5 square kilometer stationary island "aircraft carriers" in the South China Sea. This includes a 2.13 square kilometer on Woody Island on the Northern Paracel Island; a 2.74 square kilometer base on Fiery Cross Reef on the Southern Spratly Island group; a 3.95 square kilometer base on Subic Reef and a 5.58 square kilometer base on Mischief Reef. China also is trying to reclaim Mischief Reef even though it is almost 800 miles from mainland China's coast and is well within the Philippines exclusive economic zone.

When the next president takes office in January 2017, he or she will face a multitude of threats, not the least of which will be China's four stationary and one mobile aircraft carriers in the South China Sea. The Obama administration,

---

[99] "The First Sea Lord/RUSI International Sea Power Conference," *Defense Security and Equipment International (DSEI) web site*, September 14, 2015, http://www.dsei.co.uk/Content/The-First-Sea-Lord-RUSI-International-Sea-Power-Conference-1-2.

[100] Weisgerber, Marcus, "Defiant Chinese Admiral's Message: South China Sea 'Belongs to China'," *Defense One*, September 14, 2015, http://www.defenseone.com/threats/2015/09/defiant-chinese-admirals-message-south-china-sea-belongs-china/120989/.

regretfully, is not likely to change course and will continue with its failed legal and diplomatic strategy, which China will continue to ignore. During the Obama administration's remaining term, China will continue its aggressive actions to grab as much territory as possible to solidify its position in the South China Sea.

It is estimated that each of these "stationary carriers" will be capable of supporting at least 24 combat aircraft, plus associated command and control facilities to include extended range radars. Six warships will most likely be stationed at Fiery Cross Reef and up to 50 or more at Mischief Reef. China will also deploy multiple anti-aircraft missiles like the 200 kilometer range HQ-9, which was spotted on Woody Island on February 14, 2016.[101] It can be expected that China will deploy anti-ship missiles like the 400 kilometer range YJ-62. It could also deploy the 4,000 kilometer range DF-26. This intermediate range ballistic missile could reach stationed U.S. Marines in Guam and Darwin, Australia.

By the early 2020's, one or more aircraft carriers could join the Liaoning, China's first carrier. Even today, China could mobilize invasion operations of hundreds of civilian cargo roll-on/roll-off ships,[102] as it did while building its Spratly Island bases.

Chinese diplomats brag about their restraint in not using their superior naval and marine forces to capture other islands in the Spratly chain, currently occupied by the Philippines, Taiwan, and Vietnam. Capturing and building up their disputed islands would greatly facilitate China's naval and air forces to complete its control of the South China Sea. A central part of such an effort probably would be to invade the Philippine Island of Palawan. Such an aggressive and hostile act would most likely bring the U.S.-Philippines Mutual Defense Treaty[103] into play.

---

[101] Fisher, Richard D., "China deploys HQ-9 surface-to-air missiles to Woody Island," *IHS Jane's 360,* February 17, 2016, http://www.janes.com/article/58071/china-deploys-hq-9-surface-to-air-missiles-to-woody-island.

[102] Fisher, Richard D., "Ro-ro barges emerge as China's modest power-projection platform," *IHS Jane's 360,* August 13, 2015, http://www.janes.com/article/53636/ro-ro-barges-emerge-as-china-s-modest-power-projection-platform.

[103] Fact Sheet, "U.S. Relations with the Philippines," *U.S. Department of State web site*, November 13, 2015, http://www.state.gov/r/pa/ei/bgn/2794.htm.

Control of the South China Sea, aside from its security objectives, would provide China with the capability to threaten the over $5.3 trillion[104] in annual commerce that transits this critical region. Any interference with freedom of navigation affecting the region's flow of commerce would have a major global impact.

In addition, control of the South China Sea as "virtually a Chinese lake"[105] would facilitate the operation of China's nuclear ballistic missile submarines aimed at the United States.[106]

China cannot be allowed to consolidate its control of the South China Sea uncontested. This would be a dramatic reversal of U.S. strategic doctrine that would abandon America's dominant position in Asia.

In addition to China's activity in the South China Sea, it has also enabled North Korea to become a nuclear weapons state. China does not fear other Asian nations acquiring nuclear weapons. China, with its 3,000 miles of underground reinforced tunnels for its strategic forces, poses a serious nuclear threat. The former head of Russia's strategic forces, General Elden, told me that Russia estimates China has 1600-1800 ballistic missile. This is over 5 times the official U.S. estimate.

What America Needs to Do

The new President must clearly discard what NBC News special correspondent Tom Brokaw considers, the Obama administration's "benign neglect"[107] strategy and implement a robust strategy to protect U.S. strategic interests, as well as enforce our commitments to our allies. The new administration must send a clear message by deploying a combination of forces which have the capability to

---

[104] Glaser, Bonnie S., "Armed Clash in the South China Sea: Contingency Planning Memorandum No. 14," *Council on Foreign Relations*, April 2015, http://www.cfr.org/world/armed-clash-south-china-sea/p27883.

[105] Green, Michael et al. *Asia-Pacific Rebalance 2025 Capabilities, Presence, and Partnerships: An Independent Review of U.S. Defense Strategy in the Asia-Pacific,* January 2016, p. 19.

[106] Gertz, Bill, "Northcom: China's Three Missile Submarines a 'Concern'," *Washington Free Beacon*, April 7, 2015, http://freebeacon.com/national-security/northcom-china-begins-missile-sub-patrols/.

[107] Rutz, David, "Brokaw: Obama Has Shown 'Benign Neglect' Toward Islamic State," *Washington Free Beacon*, November 22, 2015, http://freebeacon.com/national-security/brokaw-obama-has-shown-benign-neglect-toward-islamic-state/.

destroy China's new man-made bases, thereby immediately raising the level of deterrence.

Accordingly, the Philippine island of Palawan must be protected and considered a top priority due to its critical position in the area. The U.S. should offer the Philippines 200 of the 300 kilometer range ATACMS short range ballistic missiles. Next, we should offer Manila a squadron of F-16 F/A-18 fighters under an innovative lend-lease program. In addition, several frigate-size combat ships should be offered, as well as stationing up to a U.S. Air Force fighter wing and combat ships at Philippine bases. Finally, amphibious exercises should also be conducted in selected adjacent islands. A combination of these actions will send the proper signal to China that their aggressive actions will not go unchallenged.

China's number one objective remains Taiwan. For the first time since the 1950's, China is approaching a serious level of preparation for an invasion of Taiwan.[108] Taiwanese analysts estimate that with combined military and civilian cargo ships and ferries, China can transport eight to 12 divisions to Taiwan[109], approaching the size of Taiwan's 130,000 man Army.[110]

The 1979 Taiwan Relations Act[111] stipulates that the President should sell defensive arms to Taiwan. The latest arms package[112] includes 500 new anti-tank and man-carried anti-aircraft missiles useful to counter invasion forces. It also includes two ASW frigates, Phalanx ship defense systems, and 36 amphibious armed personnel carriers. However, much more has to be provided. For example, assistance and systems for Taiwan's indigenous submarine program need to be provided, as well

---

[108] "Taiwan military says China preparing for possible attack," *Asia Times*, October 27, 2015, http://atimes.com/2015/10/taiwan-military-says-china-preparing-for-possible-attack/.

[109] Fisher, Richard D. and James Hardy, "China practices Taiwan invasion with civilian ferries, bomber flights in Bashi Channel," *IHS Jane's Defense Weekly*, June 16, 2015, http://www.janes.com/article/52268/china-practices-taiwan-invasion-with-civilian-ferries-bomber-flights-in-bashi-channel.

[110] "A brief comparison between the military forces of China and Taiwan," *Taipei Times*, September 23, 2011, http://www.taipeitimes.com/News/taiwan/archives/2011/09/23/2003513977.

[111] "H.R. 2479 – Taiwan Relations Act," *United States Congress web site,* March 24, 1979, https://www.congress.gov/bill/96th-congress/house-bill/2479.

[112] Brunnstrom, David and Patricia Zengerle, "Obama administration authorizes $1.83-billion arms sale to Taiwan," *Reuters*, December 17, 2015, http://www.reuters.com/article/us-usa-taiwan-arms-idUSKBN0TZ2C520151217.

as long-sought newly upgraded F-16 aircrafts to replace its aging French Mirage-2000 fighters.

We also need to look at new asymmetric capabilities for Taiwan. In that sense, U.S. defense companies are now developing new longer range and precision guided artillery shells that could turn Taiwan's 600 155-Millimeter artillery systems into potent anti-ship weapons. Such a program would better reflect Taiwan's value to U.S. strategy in Asia and significantly raise the deterrence equation with China.

CHINESE MILITARY BUILDUP

By Bill Gertz

The era of U.S. government policies designed to play down or dismiss growing strategic challenges from China seems to be ending.

For the first time in years, the nation's most senior intelligence official revealed that China now poses a regional security threat and is engaged in hostile activities that blur the line between war and peace.

In February of 2016, James Clapper, the director of national intelligence, testified before the U.S. Senate that the threat from Beijing is not limited to the large-scale buildup of both strategic nuclear and conventional forces. It includes new forms of competition involving information operations, cyber-attacks, intelligence activities and other non-kinetic forms of warfare.

Clapper warned that China, along with Russia, is challenging the U.S. for regional power and influence in ways that will increase competition, especially in vital sea lanes in Asia where trillions of dollars of commerce could be threatened.

To avoid triggering a shooting war with U.S., the Chinese are engaging in new types of low-level conflict.

"They will almost certainly eschew direct military conflict with the U.S. in favor of contests at lower levels of competition — to include the use of diplomatic and economic coercion, propaganda, cyber intrusions, proxies, and other indirect applications of military power — that intentionally blur the distinction between peace and wartime operations," Clapper said of China and Russia in his prepared statement to the Senate Armed Services Committee Feb. 9.

China Targets More than Just Taiwan

For years, military leaders insisted China's large-scale military buildup was limited to preparing for a Taiwan conflict, should China decide to retake the island by force.

Referring to the "massive" military reorganization of the People's Liberation Army announced Dec. 31, 2015, Marine Corps. Lt. Gen. Vincent R. Stewart, head of

the Pentagon's Defense Intelligence Agency, warned that China's military is "planning for U.S. intervention" in conflicts not just over Taiwan, but also in the South China and East China Seas. "China has the world's largest and most comprehensive missile force, and has prioritized the development and deployment of regional ballistic and cruise missiles to expand its conventional strike capabilities against U.S. forces and bases throughout the region," Stewart said, noting continued deployment of anti-ship ballistic missiles "to attack U.S. aircraft carriers."

Stewart also highlighted the space warfare threat posed by China that he said "possesses the world most rapidly-maturing space program" along with space weapons "designed to limit or prevent the use of space-based assets by adversaries in a crisis or conflict."

MIRVing Long-Range Ballistic Missiles

China's military has begun retrofitting single-warhead DF-5 intercontinental ballistic missiles with multiple, independently targetable re-entry vehicles, according to U.S. defense officials. The upgrading of the DF-5 missiles with multiple warheads, known as MIRVs, was detected by U.S. intelligence agencies within the past several months.

The addition of three warheads on the long-range missiles marks a significant shift for China's nuclear arsenal that is increasing in both warheads and missile systems under a major buildup.

Analysts say the warhead upgrades could affect U.S. strategic nuclear deterrence strategy by requiring a boost in U.S. warheads in the future.

Adm. Cecil Haney, commander of the Strategic Command, confirmed last month that China is making "significant investments" to both nuclear and conventional forces, including the addition of MIRVed missiles.

"China is re-engineering its long-range ballistic missiles to carry multiple nuclear warheads," Adm. Haney said Jan. 22 in a speech.

Strategic Command spokesman Lt. Col. Martin O'Donnell, however, declined to comment on the impact of the MIRVed Chinese missiles.

Additionally, China recently showed off a new DF-26 intermediate-range missile that Beijing said can be armed with either nuclear or conventional warheads. The Chinese also conducted six successful tests of a hypersonic glide vehicle.

Former Pentagon nuclear forces expert Keith Payne said the Chinese buildup highlights the failure of the Obama administration's policy of seeking to reduce global nuclear arsenals by cutting U.S. weapons.

"If China continues to modernize its nuclear forces, including the MIRVing of its long-range ballistic missiles, it will have demonstrated the utter failure of the theory that the U.S. 'moral example' of continued nuclear reductions leads to nuclear reductions globally and, ultimately, to nuclear zero," Mr. Payne told Inside the Ring.

The view that U.S. nuclear cuts promote global nuclear nonproliferation and disarmament appears to be a key tenet of U.S. strategic policy for years.

"China's nuclear weapons programs, along with Russia's, demonstrate as nothing else could the failure of that approach, and that we once again need to place priority on sustaining U.S. capabilities to deter attacks on ourselves and our allies," Mr. Payne said. "The years of America's nuclear indolence must now come to an end."

Mark Stokes, a former Air Force officer and China weapons expert, said the DF-5 upgrade and the new MIRV missiles "certainly means a significant growth in the number of nuclear warheads that can reach us here in the greater Washington, D.C., area."

Mr. Stokes, of the Project 2049 Institute, said the multiple-warhead DF-5B, an advanced variant, probably entered service several years ago, and that replacing all single-warhead, silo-based DF-5As with the multiple warheads was expected.

"Add the new mobile MIRVed ICBM to the mix, [and] this means a pretty significant growth over the next decade or so," Mr. Stokes said, noting the DF-5s likely are being upgraded from one warhead to three MIRVs.

Rick Fisher, a China military analyst, said the uploading of DF-5 warheads means the Chinese probably are deploying additional DF-5s beyond the estimated total number of 20 missiles several years ago.

"When you add the possibility of MIRVed DF-5s exceeding 20, to the imminent deployment of the road-mobile and rail-mobile MIRVed DF-41, and the potential for a MIRVed version of the DF-31 called the DF-31B, it becomes possible to consider that China may reach 500 or more ICBM warheads in the next few years," said Mr. Fisher, a senior fellow at the International Assessment and Strategy Center.

"This, combined with China's aggressive development of missile defenses, space warfare capabilities and possible non-nuclear prompt global strike missiles, will quickly undermine confidence by U.S. allies in the extended U.S. nuclear deterrent," he added.

Anti-Satellite Missiles

In 2015, U.S defense officials revealed that a test of the Dong Neng-3 missile, described as an exoatmospheric vehicle with anti-satellite strike capabilities, was carried out Oct. 30 from China's Korla Missile Test Complex in western China.

Images of contrails from the missile test were posted on Chinese websites.

Officials said the missile is the third known anti-satellite missile operational or under development by China. Earlier tests involved anti-satellite missiles known as the DN-1 and DN-2. The DN-1 has also been labeled the SC-19.

China is building anti-satellite missiles and other weapons that can destroy satellites at the highest geosynchronous orbits, some 22,000 miles above the earth. In addition to missiles, the Chinese are working on ground-based lasers and electronic jammers to disrupt or destroy satellites. Small maneuvering satellites also have been tested that are capable of grabbing and crushing orbiting satellites.

Defense officials said the Pentagon, and in particular the Air Force, are very concerned about Chinese anti-satellite weapons, that with as few as two dozen strikes could cripple the critical satellites used for communications, navigation, targeting and other strategic military functions.

During a House hearing in March, Air Force Lt. Gen. John "Jay" Raymond, commander of the Joint Functional Component Command for Space, warned that "We are quickly approaching the point where every satellite in every orbit can be threatened."

Hypersonic Glider

As noted above, China conducted six successful tests of a new high-speed hypersonic glide vehicle, the most recent in November, and also recently tested an anti-satellite missile, according to the commander of the U.S. Strategic Command.

Adm. Cecil D. Haney, the commander in charge of nuclear forces, said the tests are part of a worrying military buildup by China, which also includes China's aggressive activities in the South China Sea.

"China continues to make significant military investments in their nuclear and conventional capabilities, with their stated goal being that of defending Chinese sovereignty," Adm. Haney said during a speech to the Center for Strategic and International Studies.

"It recently conducted its sixth successful test of a hypersonic glide vehicle, and as we saw in September last year, is parading missiles clearly displaying their modernization and capability advancements," he added.

The six tests of the hypersonic glide vehicle, regarded by U.S. intelligence agencies as a nuclear delivery system designed to defeat missile defenses, were first reported by the *Washington Free Beacon*.

Defense officials said the hypersonic glide vehicle tested on Nov. 23, known as DF-ZF, was launched atop a ballistic missile fired from China's Wuzhai missile test center in central China.

The glider separated from the booster and flew at extremely high speed—between Mach 5 and Mach 10—along the edge of space.

Adm. Haney confirmed all six tests were successful, indicating the weapon program is proceeding. He described the hypersonic threat as a challenge to U.S. strategic deterrence.

The congressional U.S.-China Economic and Security Review Commission stated in its latest annual report that the hypersonic glide vehicle program is "progressing rapidly" and the weapon could be deployed by 2020.

China also is building a powered version of the high-speed vehicle that could be fielded by 2025.

"The very high speeds of these weapons, combined with their maneuverability and ability to travel at lower, radar-evading altitudes, would make them far less vulnerable than existing missiles to current missile defenses," the commission stated.

Action Items

American government officials for years have adopted an array of Chinese-style maxims that dominated public discourse on China. They included the statement from the 1990s that "China is not a threat," to the more recent iteration in the 2000s that "we want a strong China."

The new assessments are signs that the policies of the U.S. government toward China are hardening and will likely lead to concrete policy changes in the coming months.

Conciliatory U.S. policies toward China were an outgrowth of the views of many U.S. academics, public policymakers, intelligence officials and private business leaders who argued that any criticism of China, whether for its arms proliferation, human rights abuses or the military buildup, would upset trade ties and other economic relations.

The argument was made that trading with China through the years would have a moderating influence on the communist party-ruled system and ultimately produce western-style political and economic reforms.

The policies, however, so far have not produced the desired results.

Recently, U.S. intelligence leaders' testimonies appear to signal the beginning of a new era of realism toward China, which needs to continue.

In regards to MIRVing long-range ballistic missiles, the Pentagon should reverse the decision made by the George H.W. Bush administration in the 1990s to unilaterally withdraw U.S. tactical nuclear arms from U.S. ships, submarines and land-based forces in Asia. According to Rick Fisher, a China military analyst, "This will help to deter China from invading Taiwan as well as help to deter China's ally, North Korea, from using its nuclear weapons."

Regarding the United States' defense against Chinese hypersonic glide vehicles, retired Air Force Lt. Gen. David Deptula, dean of the Mitchell Institute,

said hypersonic weapons are needed to fill gaps in U.S. weapons shortfalls. Foreign hypersonic weapons also threaten all elements of military's "kill chain" used in war fighting, he said.

He added that hypersonic weapons are needed against hardened nuclear facilities, mobile missiles of other targets defended by high-technology air and missile defense.

"It's well past time for the U.S. military to get serious about developing hypersonic munitions," Deptula said.

ESPIONAGE AND CYBER: CHINA STEPS UP A COVERT WAR[113]

By Fred Fleitz

"This is the biggest vacuuming up of U.S. proprietary data that we've ever seen. It's a machine."

– Shawn Henry, former Executive Assistant Director of the FBI[114]

China has long engaged in aggressive foreign intelligence operations to advance its interests, safeguard its security, undermine its enemies and adversaries, and steal corporate secrets. While Chinese espionage in the past had often been regarded as aggressive but sloppy, that has changed in recent years. Chinese intelligence services have become more professional and technologically savvy. A massive increase in cyber warfare by Chinese intelligence agencies reportedly has allowed China to steal large amounts of American military technology, industrial technology, and the personal information of American citizens. Chinese cyber warfare also has targeted U.S. infrastructure such as the power grid.

The sharply increased pace of Chinese intelligence operations against the United States is another indication of possible conflict with the U.S. This chapter provides an overview of these operations and how the United States has responded to them.

How China Conducts Espionage

Chinese intelligence operations differ markedly from those of the United States. U.S. intelligence agencies collect information to inform policymakers on foreign policy and national security matters, not for offensive reasons or to steal economic and military secrets. By contrast, offensive intelligence operations and the theft of military and economic secrets are primary missions of Chinese intelligence.

[113] This article was submitted and cleared for classification reasons by the CIA Prepublication Review Board.

[114] Riley, Michael and Dune Lawrence, "Hackers Linked to China's Army Seen From EU to DC," *Bloomberg Business*, July 26, 2012, http://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.

China also uses intelligence operations to monitor and influence overseas Chinese populations and democracy activists.

China has several intelligence and security organizations which generally work independently of each other. Much is unknown outside of China as to how Chinese intelligence operates. In addition, The People's Liberation Army (PLA) conducted major reforms announced on December 31, 2015, which will affect the structure, mandate, and wiring diagram of China's intelligence organizations. Prior to these reforms, the main Chinese government entities currently engaged in foreign intelligence were:

- **Ministry of State Security (MSS)**. China's main agency responsible for intelligence and state security, in charge of counterintelligence and foreign intelligence (but not military intelligence). According to the Federation of American Scientists, the MSS is organized on the model of the old Soviet KGB, with a First Bureau dealing with domestic security and the Second with foreign services and counterintelligence. Other sections deal with signals intelligence (SIGINT) and counter-surveillance, or focus on outer territories like Taiwan.
- **Ministry of Public Security (MPS**). Conducts internal security, responsibilities include: maintenance of social order, counterterrorism, management of assemblies, processions and demonstrations, etc.
- **Second Department of the PLA General Staff Headquarters (2PLA)**. Responsible for collecting military intelligence via human intelligence (HUMINT), SIGINT, and imagery intelligence. 2PLA deploys officers to embassies and consulates overseas, as well as to Chinese state-owned enterprises, banks, and think tanks. The 2PLA may also have some responsibility for China's spy satellites.
- **3PLA**. Equivalent to the U.S. National Security Agency (NSA). 3PLA is tasked with monitoring and analyzing much of the world's communications, including: embassy cables, corporate emails, and criminal networks—for foreign threats and competitive advantages.
- **4PLA**. Responsible for Electronic Intelligence (ELINT), information derived primarily from electronic signals that do not contain speech or text; and Electronic Warfare, focused energy, usually radio waves or laser light, to confuse or disable an enemy's electronics, including electromagnetic pulse weapons.
- **PLA Unit 61398**. A shadowy organization that is believed to be the lead Chinese government unit responsible for offensive cyber warfare.

> According to a 2013 report by the U.S. cyber security firm Mandiant, Unit 61398 has systematically stolen hundreds of terabytes of data from at least 141 organizations across 20 industries worldwide since as early as 2006.[115] Mandiant estimates Unit 61398 has more than 1,000 computer servers and between hundreds and thousands of staff. According to the New York Times, NSA and other U.S. intelligence agencies have been tracking more than 20 hacking groups in China, over half of them PLA units.[116]

After the reorganization, these entities still exist, but they are now consolidated with increased funding and functionality.

The new Strategic Support Force (SSF), according to China analysts, now contains: the cyber force, which consists of "hacker troops" in charge of cyber offense and defense; the space force, which manages surveillance and satellites; and the electronic force, which is responsible for "denial, deception, disruption of enemy radars and communications systems."[117] This new force has become highly important in the PLA; it is in equal standing to China's army, navy, air force, and missile services.

> [The Strategic Support Force includes] the 3rd Department, or 3PLA, that is believed to have as many as 100,000 cyber warfare hackers and signals intelligence troops under its control. The group includes highly-trained personnel who specialize in network attacks, information technology, code-breaking, and foreign languages…. The 3PLA was identified by the National Security Agency as one of China's most aggressive cyber spying agencies.
>
> The 4th Department, China's separate military electronic intelligence and electronic warfare service…. Additionally, the traditional military spy

[115] "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant Intelligence Center Report*, March 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
[116] Perlroth, Nichole, "Questions Remain After Chinese Hacking Indictments," *New York Times*, May 19, 2014, http://bits.blogs.nytimes.com/2014/05/19/questions-remain-after-chinese-hacking-indictments/.
[117] Raska, Michael, "PLA reforms: Toward winning 'informationised local wars," *The Interpreter*, February 3, 2016, http://www.lowyinterpreter.org/post/2012/02/03/PLA-reforms-Toward-winning-informationised-local-wars.aspx.

service devoted to human spying known as 2PLA was combined into the new support force. [118]

This reorganization, specifically the prominent emphasis on space, cyberspace, and intelligence, ultimately moves towards the goal of achieving information dominance (*zhi xinxi quan).* The PLA believes its strength and ultimate victory can be achieved by maintaining information dominance. They are now taking the correct steps towards this by strategically reorganizing the military to more efficiently utilize cyberspace and intelligence-gathering for their benefit.

Cyber Theft by Chinese Intelligence

Cyber warfare to steal U.S. economic, government, and military secrets is the most well publicized sign of increased Chinese intelligence operations against the United States.

China has been rapidly developing its cyber warfare capabilities. There are three general types of cyber threats coming from China. First, the PLA has played an important role in Information Warfare (IW) since 1997. IW from the PLA relating to computers and the Internet has developed along two paths: Cyber/Internet Warfare and Cyber Intelligence and Espionage. Alongside PLA efforts are cyber threats from citizens with Internet connections who regularly use the web. These groups generally have conducted the third main cyber threat coming from China – hackers who engage in economic espionage.

The PLA has conducted extensive training and allocated significant resources in time, personnel, and monetary expenditures in developing cyber warfare capabilities since around 2000.

Cyber warfare is defined by activities that are conducted during PLA combat operations. This type of combat is intended to "damage or destroy enemy network elements, such as web sites, hard drives, operating systems and servers, as well as

[118] Gertz, Bill, "Chinese Military Revamps Cyber Warfare, Intelligence Forces: Changes meant to improve PLA high-tech warfighting," *Washington Free Beacon*, January 27, 2016, http://www.freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/.

infrastructure dependent upon those elements, such as communications systems, financial services, power grids, air traffic control systems, etc."[119]

Training for PLA cyber combat has been extensive and increasingly complex for years. The frontline cyber battle units have been reconstituted from exclusively conducting simple information warfare tactics to be reorganized into elite squadrons of "Integrated Network Electronic Warfare" combatants.

These new PLA "cyber warriors" are trained according to their cyber-attack specialties in at least 12 different training and doctrine centers throughout the country. The units are periodically invited to a "flagship" facility thought to be located in the Beijing Military Region to test their mettle in realistic war games. The flagship facility has been identified and named as the Beijing North Computing Center that coordinates PLA cyber activity according to an October 2012 report by the Project 2049 Institute, a think tank on Far East security issues.[120] The think tank believes the Beijing North Computing Center is located near Beijing University.

During cyber war games, combatant trainees serve on an attacking "Blue Force" or a defending "Red Force." They ply their trade and hone their skills in these games and approach the exercises as if they are in a realistic wartime scenario with clear winners and losers. Trainees serve on different teams and receive cross-training in many different types of cyber warfare specialties. When they return to their assigned unit, their skills are finely sharpened and they then have the ability to pass on their expertise to fellow soldiers. Subsequent training rotations lead to the dissemination of the latest hacking techniques from the most senior noncommissioned officer to the least experienced private. PLA training and doctrine development is then able to utilize the most intricate and malicious code that is available at any given time and immediately put it to use.

These field exercises and war games include "obtaining passwords, breaking codes, and stealing data; using information-paralyzing software, information-blocking

---

[119] Ball, Desmond, "China's Cyber Warfare Capabilities." *Security Challenges*. Winter 2011: Vol.7, No. 2, p. 85.

120 Gertz, Bill, "Cyber Spies Spotted – Report: Chinese Military Cyber Warfare Units Identified." *Washington Free Beacon*, October 26, 2012, http://freebeacon.com/politics/cyber-spies-spotted/.

software, information-deception software, and other malware; and developing software for effecting counter-measures."[121] Attacks have been simulated against targets in Taiwan, India, Japan, South Korea, of course, the U.S. and Europe. Key goals and objectives for these attacks focus on disabling enemy command and control networks at the beginning of hostilities or sending attacks that would disrupt a civilian power grid to provoke mass hysteria in the enemy's civilian population.

PLA Integrated Network Electronic Warfare units depend on three main capabilities: denial of service attacks, viruses, and Trojan horses. Denial of service or distributed denial of service attacks consist of interrupting, crashing, or suspending a web site, server, or router. Viruses or worms can take control of operating systems to steal or destroy information; attempt to disable or break hard drives; hijack the computer; or paralyze or make the device inoperable. Trojan horses can be inserted into a network, server, or device to destroy, damage, or hijack a single work station or thousands of personal computers in a network. PLA hackers can also plant "sleeper" Trojan horses into enemy systems during peacetime and remotely activate them during times of war.

In addition to preparing for cyber warfare, PLA Integrated Network Electronic Warfare units also concurrently take part in cyber-intelligence or espionage operations during peacetime against many different countries. These are not drills or exercises, but real world hacking that has done extensive damage over the years. The PLA is also believed to supervise or in other ways direct hackers from the People's Republic of China (PRC) intelligence agencies. The PLA additionally has reserve, auxiliary, or militia cyber espionage units that have been known to commit attacks.

Two Main Chinese Hacker Groups Target Corporations

"Byzantine Hades" was the term the Pentagon and U.S. organizations used to describe cyber espionage threats from the PLA and their proxy groups of hackers who targeted America from about 2008 to 2011. However, now there are two main Chinese citizen organizations that have emerged to conduct the most harmful attacks

121 Ball, p. 84.

against U.S. corporations, both named for the source code in which those hackers use in their malicious software.

These two largest hacker groups make up 90 percent of economic espionage against American industry. The attacks against these companies are too numerous to list, but most are members of the Fortune 500 and they span across many sectors, including: Google, Intel, Hewlett-Packard, Yahoo, Xerox, Lockheed Martin, Marriott International, Pfizer, Boston Scientific, and Abbott Laboratories. Many hacking victims do not report cyber espionage to the Federal Bureau of Investigation (FBI) or to the media.

Members of the first group, called the "Comment Gang," are believed to be primarily from Shanghai and documents gleaned from various WikiLeaks dumps have fingered the criminal ring as a proxy for the PLA. The Comment Gang's name is derived from their signature coding language that exploits targeted web page hacks that use malware to tunnel in through the "comment" section of various web sites.

Attacks from the Comment Gang date back to 2002 by some estimates. Ray Mislock, a former security expert for DuPont Co., believes the gang has targeted more than 1,000 organizations worldwide over three years. The Comment Gang has targeted U.S. energy companies, banks, pharmaceutical firms, and nongovernmental organizations such as the United Nations and the International Olympic Committee. For example, Comment hackers go after oil companies for drilling research and data on seismic maps for crude reserves and future plays. They hit investment banks for pricing trends on assets and information on strategic portfolio decisions.

The Comment Gang targets senior executives' personal computers for their emails and sensitive documents. A popular Comment Gang technique is to overwhelm, infect, and occupy a seemingly innocuous web site and wait for unsuspecting users to browse and land on the pages where malware is waiting for the victim. "Back door" vulnerability is immediately found on the target's computer and then a particularly ferocious Trojan horse scampers into the host and takes over to steal valuable files. These assaults are called "watering hole" attacks because they simulate a predator, such as a lion, who waits for targets of opportunity to visit watering holes so the predator can ambush their prey.

The Comment Gang is suspected of striking a nuclear power plant in California in 2011 and commandeering the computer of one of the corporation's strategic planners.

Sometimes political events inspire the Comment hackers. The crew once targeted EU Council President Van Rompuy, considered a key figure during the Euro zone debt crisis, and placed a "cyber wiretap" on his computer. The tap reportedly monitored his emails for at least ten days in the summer of 2012. The hackers then infected other EU council computers and stole multitudes of member emails.

The second main group, called the "Elderwood Gang," has been documented extensively by cyber security giant Symantec.[122] The moniker for these outlaws is from the term "Elderwood" which shows up repeatedly in the hackers' source code. Based in Beijing, Elderwood is known for its use of "zero day exploits." Zero day refers to malware that exploits an unknown vulnerability in a system or web site.[123] "Zero" means that security systems have never seen the attack before. Zero day malicious code is considered extremely valuable to hackers and the Elderwood Gang has the capability of manufacturing their own zero day malware and viruses. They will also habitually buy additional zero day codes over the black market from other hackers around the globe.

The Elderwood Gang specializes in defense and military hacking and will target prime contractors and their suppliers. Elderwood uses watering hole attacks in an attempt to infect entire defense supply chains, including: shipping, aeronautics, energy, manufacturing, engineering, and electronic firms in the sector.[124] Employees in any of these types of companies could browse an infected watering hole site and find an Elderwood "I-Frame" string of malicious code that will allow a hacker to hijack the victim's work station to steal emails and sensitive documents. Elderwood then waits for computers belonging to the whole supply chain to spread the virus until it reaches the prime contractor.

---

[122] O'Gorman, Gavin and Geoff McDonald. "The Elderwood Project." *Symantec Security Response*. September 7, 2012, http://www.symantec.com/connect/blogs/elderwood-project.
[123] O'Gorman and McDonald, p. 2.
[124] Ibid, pp. 3-4.

Elderwood also uses old-fashioned "spear phishing" attacks which comprise of emails that include a link or file attachment which releases the Zero day code.[125]

Some cyber security experts have pointed out that hacking events from Chinese gangs coincide with various PRC five year economic strategic plans. These attacks show links between cyber espionage activities and PRC economic policy. Consulting firm KPMG reported on the latest five year economic plan from China. It included industry targets, such as: clean energy, biotechnology, advanced semiconductors, information technology, advanced manufacturing, aerospace, telecommunications, and drugs and medical devices.[126] The Comment Group, Elderwood Gang, and other Chinese hackers have all targeted these industry sectors.

Overall, cyber threats from Chinese intelligence have been extensive, varied, imaginative, and extremely damaging. U.S. Representative Mike J. Rogers (R-MI), chairman of the House Permanent Select Committee on Intelligence, claimed in 2011 that China is "stealing everything that isn't bolted down, and it is getting exponentially worse."[127]

On May 19, 2014, the U.S. government indicted five Chinese military hackers working in Unit 61398 for economic espionage and identity theft among other crimes. These hackers targeted a solar power manufacturer, stole nuclear technology from electrical provider Westinghouse Electric Company, and obtained inside information to give a Chinese company an advantage in negotiations with Westinghouse. Chinese officials denied the charges and repeated their claim that China does not engage in hacking or cyber espionage.

Cyber Thefts of U.S. National Security Secrets

A special focus of Chinese cyber theft has been stealing U.S military and intelligence secrets. In a January 2015 *Washington Free Beacon* article, reporter Bill Gertz said that sensitive technology and aircraft secrets stolen by Chinese hackers

[125] O'Gorman and McDonald, p. 3.
[126] Riley, Michael and John Walcott. "China-Based Hacking 760 Companies Shows Cyber Cold War." *Bloomberg Business*, December 14, 2011, http://www.bloomberg.com/news/articles/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.
[127] Ibid.

eight years ago, have been incorporated into China's new J-20 stealth fighter. According to Gertz, "by learning the secrets, the Chinese were able to include the design and technology in Beijing's new stealth jet, the J-20. The secret also could allow Chinese air defenses to target the F-35 in a future conflict."[128]

According to a May 2013 Defense Science Board report, the designs of more than two dozen major weapons systems have been comprised by Chinese hackers. Also in 2015, the Obama admin charged Chinese hackers with trying to steal information on the C-17 cargo plane and the F-11 fighter.[129]

On October 8, 2012, the House Intelligence Committee issued a bipartisan unclassified report[130] warning U.S. companies considering doing business with Chinese telecommunications companies Huawei and ZTE, to find another vendor because of the likelihood that both companies are cooperating with the Chinese government on cyber espionage.

Chinese cyber-attacks against the U.S. government include a breach at the U.S. Office of Personnel Management in 2015 which may have compromised the personal information of 21.5 million government workers. This was valuable data for Chinese intelligence since it could be used to sift through personnel records of State Department employees to determine those at the U.S. embassy in Beijing who were Department employees and others who actually work for U.S. intelligence agencies. As a result of this breach, the Central Intelligence Agency (CIA) pulled several of its officers out of the embassy in September 2015, according to the Washington Post.[131]

---

[128] Gertz, Bill, "NSA Details Chinese Cyber Theft of F-35, Military Secrets," *Washington Free Beacon,* January 22, 2015, http://www.freebeacon.com/national-security/nsa-details-chinese-cyber-theft-of-f-35-military-secrets/.

[129] Nakashima, Ellen, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post,* May 27, 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html.

[130] Phalen, Susan and Heather Moeder Molino, "Chairman Rogers and Ranking Member Ruppersberger Warn American Companies Doing Business with Huawei and ZTE to 'use another vendor'," *U.S. House of Representatives Permanent Select Committee on Intelligence website,* October 8, 2012, https://intelligence.house.gov/press-release/chairman-rogers-and-ranking-member-ruppersberger-warn-american-companies-doing.

[131] Nakashima, Ellen and Adam Goldman, "CIA pulled officers from Beijing after breach of federal personnel records," *The Washington Post*, September 29, 2015,

This hack also may have damaged U.S. national security because the stolen data included information from U.S. government forms used for security clearances, known as SF86 questionnaires.

The U.S. government hinted that China was behind this cyber attack but never directly accused Beijing. The Chinese government has vehemently denied it engages in state-sponsored cyber warfare. In December 2015, Chinese officials announced that after an investigation it had determined the OPM hack was a criminal case and made several arrests.

Another instance of China targeting U.S. government computers, according to a 2008 report, is when Chinese hackers broke into the computers of former Congressman Frank Wolf (R-VA). Wolf claims that his office was targeted because he was a vocal critic of Chinese human rights violations and his many relationships with Chinese dissidents and refugees.[132]

There also was a report in 2011of a massive penetration into the computers of the U.S. Chamber of Commerce by hackers linked to the Chinese military. [133]

Chinese cyber warfare has had serious implications for U.S. national security. According to a January 17, 2015 '60 Minutes' report:

> The Justice Department says that the scale of Chinese corporate espionage is so vast that it constitutes a national security emergency, with China targeting virtually every sector of the U.S. economy, and costing American companies hundreds of billions of dollars in losses – and more than two million jobs.[134]

Russia and China have both allegedly conducted cyber warfare targeting U.S. infrastructure. According to an April 8, 2009 Wall Street Journal article, spies from

---

https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html.

[132] Somashekhar, Sandhya, "Wolf Warns of Foreign Attacks on Computers," *The Washington Post,* June 12, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061102790.html.

[133] Gorman, Siobhan, "China Hackers Hit U.S. Chamber: Attacks Breached Computer System of Business-Lobbying Group; Emails Stolen," *The Wall Street Journal*, December 21, 2011, http://www.wsj.com/articles/SB10001424052970204058404577110541568535300.

[134] Stahl, Leslie, "The Great Brain Robbery," *CBS News.com*, January 17, 2016, http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/.

Russia, China, and other countries reportedly "have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system." Foreign infiltration of the U.S power system is not fully understood, however, according to a senior intelligence official, "The Chinese have attempted to map our infrastructure, such as the electrical grid . . . So have the Russians."[135]

Admiral Michael Rogers, head of the NSA and the U.S. Cyber Command, also warned about this threat in 2014 when he testified to the House Intelligence Committee. He relayed that China and perhaps two other unnamed nations had "the ability to launch a cyber-attack that could shut down the entire U.S. power grid and other critical infrastructure."[136]

Non-Cyber Intelligence Collection and Operations

China's recently improved intelligence operations have included other efforts, many using traditional intelligence methods. CNN reported in August 2015 that U.S. officials said the number of Chinese government secret agents in the U.S. has spiked.[137] Most enter the U.S. on tourist or business visas without declaring themselves as required under U.S. law. According to the CNN report, these officers are conducting covert Chinese law enforcement on U.S. soil and pressure Chinese citizens to return to China to face justice, often on corruption charges. The U.S. government has protested the illegal entry into the United States by PLA officers and their efforts to intimidate Chinese citizens to return to China.

It is very likely that officers of other Chinese intelligence agencies are also operating in the United States in significant numbers. In addition to those who enter the United States with tourist or business visas, some also enter the United States under diplomatic cover with the Chinese embassy, Chinese consulates, and international organizations like the United Nations.

---

[135] Gorman, Siobhan, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://www.wsj.com/articles/SB123914805204099085.

[136] Lenzener, Robert, "Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid," *Forbes.com*, November 28, 2014, http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber-attack-could-shut-down-u-s-electric-power-grid/#9a0a4b9479f5.

[137] Sciutto, Jim and Eugene Scott, "U.S. officials: Chinese secret agents in U.S. spikes," *CNN*, August 19, 2015, http://www.cnn.com/2015/08/19/politics/chinese-spies-double-digits/.

Possible expanded Chinese intelligence operations in the United States will likely attempt to repeat its successes of the past, which included, according to the 1999 Cox Committee report, stealing the blueprints for seven of America's nuclear warheads, including the neutron bomb, the W-88 nuclear warhead and plans for America's Trident, Minuteman, Lance, Peacekeeper missiles.[138]

There are indications that Chinese intelligence operations have become increasingly bold in recent years. According to an April 26, 2014 Sydney Morning Herald article, Chinese intelligence is building covert networks of informants at leading universities in Melbourne and Sydney to keep tabs on ethnic Chinese lecturers and students. China is reportedly engaged in similar efforts in other countries, including the United States.[139] Xia Yeliang, a prominent Beijing scholar who fled to the United States in 2014, warns that China has also been sending spies to American universities and urges U.S. institutions to tread carefully on academic co-operation.[140]

Intensified Chinese efforts to recruit American students to spy for China led the FBI in 2014 to make a video warning Americans studying in China not to be recruited as Chinese spies.[141] This video was made in the aftermath of the arrest of Glenn Duffie Shriver, a former American student who studied in China. In 2010, Duffie, age 24, was sentenced to four years in prison for conspiring to spy for China by attempting to win employment with the U.S. State Department and the CIA.[142]

---

[138] "Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China," *U.S. House of Representatives*, January 3, 1999, http://www.house.gov/coxreport/cont/gncont.html.

[139] Garnaut, John, "China spreads its watching web of surveillance across Australia," *Sydney Morning Herald*, April 26, 2014, http://www.smh.com.au/national/china-spreads-its-watching-web-of-surveillance-across-australia-20140425-379om.html.

[140] Agency France Press Report, "Chinese 'spies' attending US universities, says expelled Peking University professor," *China South Morning Post,* February 28, 2014, http://www.scmp.com/news/china/article/1437005/expelled-peking-university-professor-warns-us-universities-over-educating.

[141] Raujala, Emily, "FBI Movie Warns U.S. Students Not to Spy for China," *Time*, April 16, 2014, http://time.com/64530/fbi-movie-game-of-pawns-china/.

[142] Taylor, Adam "A cheesy FBI video hopes to stop U.S. students from becoming Chinese spies," *The Washington Post*, April 15, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/04/15/a-cheesy-fbi-video-hopes-to-stop-u-s-students-from-becoming-chinese-spies/.

According to Assistant U.S. Attorney Stephen Campbell, the Duffie case was unique because the Chinese government has previously never recruited an American citizen as a spy and tried to plant him inside the CIA.[143]

These instances are likely just the tip of the iceberg of a huge increase in Chinese intelligence operations in the United States. There may have been a good indication of this in 2008, the year of the Beijing Olympics, when China organized large numbers of pro-China demonstrators to protect the Olympic torch relay in San Francisco in 2008. According to a STRATFOR report[144], the Chinese government organized a massive pro-China presence to prevent anti-China demonstrators from putting out the torch in San Francisco as they had done in other cities. The pro-China demonstrators were disciplined and may have engaged in intelligence collection against the anti-China demonstrators. They also attempted to provoke anti-China demonstrators into performing acts of provocations which could be photographed to discredit the anti-China argument. The STRATFOR report added:

> "China has had a long reach into the Chinese community in the United States for quite some time, and frequently uses this community for espionage, both within the community itself and against American companies, the military and the technology and political spheres. Also, Chinese consulates in the United States have helped facilitate pro-China gatherings in the past. However, while it already was known that China was anxious to restore its image after the Tibet unrest and the trouble with the torch run in London and Paris, the effort and coordination Beijing exhibited in San Francisco, through the consulate and local Chinese business and social organizations, was rather impressive." [145]

An Inadequate U.S. Government Response

Despite growing evidence of greatly improved Chinese intelligence and cyber operations against the United States, the response by the U.S. has been woefully

[143] Wise, David, "Mole-in-Training: How China Tried to Infiltrate the CIA," *Washingtonian*, June 7, 2012, http://www.washingtonian.com/2012/06/07/chinas-mole-in-training/.
[144] "China: The Olympic Torch Obstacle Course," *STRATFOR*, March 24, 2008, https://www.stratfor.com/analysis/china-olympic-torch-obstacle-course.
[145] "Beijing's Obvious Hand at the US Olympic Torch Run," *STRATFOR Security Weekly*, April 16, 2008, https://www.stratfor.com/weekly/terrorism_weekly_april_16.

inadequate. Condemnations of Chinese intelligence operations in the United States by the Bush and the Obama administrations have been rare and muted.

While the Obama administration has clearly paid little attention to Asia, it has made improving China a priority of its Asia foreign policy. For this reason, Obama officials have avoided criticizing China for the large number of China-linked cyber warfare incidents that occurred during the Obama years.

An important exception was when the U.S. indicted five members of Unit 61398 in 2014 for hacking U.S. corporations.

Despite the 2014 indictments and press reports of ongoing Chinese government hacking of U.S. government and corporate computers, President Obama signed an agreement with Chinese leader Xi Jinping on September 25, 2015 in which both governments pledged not to conduct or condone economic espionage in cyberspace. This was considered a laughable agreement by many experts because it only barred China from conducting economic espionage but not hacking with intent to steal military and intelligence secrets. The agreement also handed Xi a major propaganda win due to the press conference he did on this agreement with President Obama, during which Xi yet again denied that China conducts economic cyber warfare.

The next month, U.S. cyber security firm CrowdStrike reported that China had already broken this agreement with cyber-attacks against U.S. technology and pharmaceutical companies to steal intellectual property.[146] This report validated the concerns of Director of National Intelligence James Clapper, who testified to the Senate Armed Services Committee on September 29, 2015.[147] Clapper was skeptical of the U.S.-China cyber agreement's ability to slow a growing torrent of Chinese cyber-attacks on U.S. computer networks.

In 2009, the Pentagon created the U.S. Cyber Command to defend Department of Defense networks, systems and information, to defend the homeland

[146] CBS News, "China already violating U.S. cyber agreement, group says," *CBS News.com*, October 19, 2015, http://www.cbsnews.com/news/crowdstrike-china-violating-cyberagreement-us-cyberespionage-intellectual-property/.
[147] Mehta, Aaron, "Clapper Sceptical of US-China Cyber Deal," *Defense News*, September 29, 2015, http://www.defensenews.com/story/defense/policy-budget/cyber/2015/09/29/clapper-skeptical-us-china-cyber-deal/73027008/.

against cyberattacks, and to provide support to military and contingency operations. U.S. intelligence agencies have increased their efforts to counter cyber warfare. In 2015, the Office of the Director of National Intelligence created the Cyber Threat Intelligence Integration Center. However, although Cyber Command was supposed to have 6,000 employees, it had only about half that number by early 2015.[148]

The CIA created its own large cyber operations division, the Directorate of Digital Innovation, in the fall of 2015.

The success of these cyber security intelligence organizations is still uncertain. There also are questions as to whether these competing cyber intelligence organizations will cooperate with one another.

While the FBI made the aforementioned video warning U.S. students not to spy for China, it appears the Obama administration has taken no serious steps to counter increased Chinese intelligence operations in the United States. Moreover, the FBI film does not appear to have been taken seriously by the press and was mocked as "cheesy" by the *Washington Post*.[149]

The Bottom Line

China has a determined and expanding intelligence effort against the United States to advance its military and economic power which U.S. officials have underestimated and done little to counter. The pervasiveness of these intelligence operations could go beyond transforming China into an economic and military superpower – they could represent a comprehensive and gradual program to prepare for a future war with the United States.

To assess this threat, a new bipartisan congressional commission like the 1998-1999 Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China (the Cox Committee) should be formed. This commission could conduct an investigation, hold hearings, issue a report

[148] Sternstein, Aliya, "US Cyber Command Has Just Half the Staff It Needs," *Defense One*, February 8, 2015, http://www.defenseone.com/threats/2015/02/us-cyber-command-has-just-half-staff-it-needs/104847/.

[149] Taylor, Adam, "A cheesy FBI video hopes to stop U.S. students from becoming Chinese spies," *The Washington Post*, April 15, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/04/15/a-cheesy-fbi-video-hopes-to-stop-u-s-students-from-becoming-chinese-spies/.

on Chinese intelligence, cyber and military threats, and make policy recommendations for the next president.

This commission should also conduct an assessment on the damage to U.S. national security from Chinese-stolen U.S. military secrets. They should also assess the threat posed to U.S. homeland security by China's targeting of America's infrastructure and increased Chinese intelligence operations within the United States.

PROSPECTS FOR EXTENDED DETERRENCE IN SPACE AND CYBER: THE CASE OF THE PRC

By Dean Cheng

The diverging political context for providing what is known as "extended deterrence" in the Asian Pacific region, coupled with China's perspectives on extended deterrence in outer space and cyberspace, has important implications for the United States. American deterrence focuses on dissuasion, seeking to influence opponents to avoid actions that would harm American interests. China sees deterrence as not only dissuasive, but also coercive, as a way to persuade opponents to follow actions that further Chinese objectives. China, given its lack of allies, engages in direct deterrence but also counters extended deterrence, since its coercive actions against Japan, for example, would require that dissuasive action be taken against the United States. For the United States, the issue in the Asia–Pacific is not direct deterrence versus extended deterrence. China will assess all American actions to grasp the essence of American deterrence, employing its diverse forces to signal its resolve and intentions.

While there has been discussion about whether today's security environment constitutes a "neo-Cold War," the reality is that it is actually more complex than the Cold War. For most of the period between 1947 and 1992, the situation was largely marked by a bipolar balance, where the two major players created somewhat symmetrical blocs of allies, friends, and client states. Consequently, there was a potential for symmetric responses and signaling. As important, there was a perceived continuum of security that spanned conventional and nuclear thinking, linking the use of force in the former to the potential for escalation into the latter. It is within this context that "extended deterrence" took shape.

Today's world, however, is much more multipolar, so most states, including increasingly the U.S., have to consider more than just a single, highest priority contingency. Consequently, signaling is also more difficult, especially because there is no symmetry of relations and alliance networks. This is exacerbated by the spread of military operations to outer space and the cyber realm. That various activities are

more open to consideration in space and cyber erodes the conceptual firebreak that marked the Cold War.

It is important to begin with some definitions of key concepts. First, what is deterrence? From the American perspective, deterrence is the combination of actual capability and will to employ that capability to influence an adversary, typically to not do something. As Alexander George and Richard Smoke wrote in 1974, deterrence "in its most general form …[is] simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits."[150]

Thus, deterrence is typically seen by American decision-makers as a goal. Although there is nothing in this formulation that presupposes deterrence as being dissuasive versus coercive, in the Western conception, deterrence is almost wholly associated with the idea of dissuasion.

This focus on dissuasion and defense, especially when it comes to space and cyber, is reflected in the array of U.S. government strategic documents including the National Security Space Strategy, the National Space Policy, the U.S. National Security Strategy, and the U.S. National Military Strategy. The American focus seems to be on deterrence in space—in particular, on deterring an opponent from attacking our own space assets. The same sort of logic appears to be developing regarding cyber, as reflected in the recent Department of Defense Cyber Strategy and the earlier Comprehensive National Cybersecurity Initiative.

In each of these respects, the People's Republic of China has a very different perspective. Whereas for the United States the very act of deterring an opponent or multiple opponents from acting in certain ways is seen as serving U.S. interests, deterrence in the Chinese view is a means rather than an end. This is because the Chinese concept of *weishe*, which is typically translated as "deterrence," embodies both "dissuasion" and "coercion." Coercion, in turn, is typically in the service of some other goal: One does not simply coerce an adversary; one coerces an adversary to get them to do something that one wants. Thus, the Chinese would employ *weishe* as the

[150] Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 11.

means, whether dissuasive or coercive, to persuade an opponent to follow a course of action that accords with larger Chinese strategic objectives.

Within such a framework, the Chinese are not necessarily interested so much in deterrence in the space or cyber environments, but rather are interested in the use of space and/or cyber as means to effect deterrence, including coercion. Thus, in Chinese writings, space operations are characterized as contributing to an effort to achieve overall goals, whether in conjunction with conventional and/or nuclear operations or on their own, either through *weishe* (i.e., dissuasion and coercion) or in actual combat. There is little discussion of deterring actions in space.

The realm of cyber would seem to be even more complex. Operations in the cyber domain are part of the larger portfolio of information operations, which includes not only what the U.S. has typically termed computer network exploitation, computer network attack, and computer network defense, but also electronic warfare; psychological operations; camouflage, concealment, and deception; and kinetic attacks against sensors, information and communications networks, and command and control facilities. While Chinese analysts have discussed "information deterrence," there appears to have been little discussion of "network deterrence" or "cyber deterrence."[151]

This, again, would seem consistent with the Chinese focus on deterring, including coercing, an adversary through actions in the information domain but not deterring actions in that domain in the first place.

These asymmetries in perspective and definition make comparisons of American and Chinese approaches to even basic deterrence approaches difficult. For the Chinese, for example, actual use of space weapons is the highest rung of what seems to be an "escalation ladder" of deterrent actions. This would seem to be a radically different perspective from that of the United States, where weapons use is rarely considered part of deterrence. This divergence holds dangerous implications in event of a crisis.

[151] It is noteworthy that there is no entry for either "electronic deterrence" or "network deterrence" in the Chinese volume of military technology.

The situation with extended deterrence is even more problematic. During the Cold War, both the United States and the Soviet Union had allies and commitments outside their national territories. Consequently, there were at least some parallels in terms of understanding extended deterrence. In the case of the PRC, however, that nation has few allies; neither Pakistan nor North Korea, the closest analogues, is comparable to the American relationship with Japan or Great Britain. Consequently, China does not have a parallel experience with extended deterrence; it is not attempting to defend allies. Instead, along its periphery, China itself directly confronts American friends and allies, whether it is Japan, South Korea, the Philippines, Thailand, or Taiwan.

This creates substantially different, asymmetric concerns between China and the United States. Where Beijing is concerned about direct deterrence (i.e., direct threats to China), Washington is engaged in extended deterrence in support of allies.

This is further exacerbated by the nature of many of the tensions. Whether it is the Senkakus dispute with Japan, the issue of Taiwan, or the South China Sea, Beijing sees these as matters of Chinese territorial sovereignty, what is often termed "core interests." Thus, China is seeking to engage in *weishe* (whether dissuasion or coercion) over territorial concerns to which the United States is not a party.

Beijing arguably perceives these concerns as defensive and preserving the status quo (i.e., its territorial integrity and sovereignty), which casts a different light again on the objectives being served by *weishe*. Deterring threats to one's own immediate territory typically embodies greater commitment and resolve.

The Problem of Extended Deterrence Through Cyberspace and Outer Space

All of these conditions make traditional extended deterrence with land, sea, and air forces difficult. The incorporation of cyberspace and outer space, however, does not necessarily mark a qualitative change in terms of deterring broad military threats to American allies.

Indeed, given the Chinese view that future "local wars under informationized conditions" will be joint operations involving operations on land, sea, and air, in outer space, and in the electromagnetic spectrum, including cyberspace, the PRC views

future *weishe* requirements in a way that resembles "extended cross-domain deterrence." That is, the PRC will seek to employ all the various forces and capabilities in pursuit of its ends; therefore, the United States should be thinking about extended deterrent measures that similarly embody all of its capabilities, including land, sea, air, outer space, cyber, and nuclear forces.

Should the PRC threaten to engage in broad actions against an ally or friend, it is not clear that the extended deterrent challenges confronting the United States would be fundamentally different because of the added domains of outer space and cyberspace.

The more difficult, but arguably the most unlikely, contingency is that of engaging in extended deterrence in the face of attacks only in cyber (or space), although it should be noted that Chinese military writings suggest that, in the event of conflict, it is unlikely that the Chinese would engage only in cyber (or space) attacks. Moreover, this presumes that there is a level of confidence in attribution such that the United States (and its allies) could be sure that it was retaliating against the right adversary.

Nonetheless, various conditions make extended deterrence in outer space and cyberspace almost impossible. To begin with, it is unclear what one wishes to deter. In the case of cyberspace, for example, if the objective is to engage in extended deterrence against computer network exploitation and cyber espionage, it is an open question how well one can defend one's own networks, never mind others'. Nor is it clear how one can credibly provide extended deterrence if the supported state should have only weak protections for its cyber systems and information infrastructure.

Indeed, the lack of American reaction in the wake of the hacking of the OPM suggests that even basic deterrence (or defense) in cyberspace is difficult.[152] This is made even more problematic by the extensive Chinese sales of

[152] Ellen Nakashima, "U.S. Decides Against Publicly Blaming China for Data Hack," *The Washington Post*, July 21, 2015, https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html?hpid=z1 (accessed October 15, 2015).

hardware to various states: How does one help defend a nation's information systems if they have embedded vulnerabilities?

Similarly, it is difficult to imagine that one can engage in extended deterrence on behalf of an ally's space assets in the face of jamming, dazzling, or other interference. As with cyber, there is an attribution issue: Was the use of a laser against a satellite an attempt to interfere with its systems or an attempt to determine its distance? As with cyber, there is also the question of an appropriate response. Barring sustained jamming and dazzling, any response will suffer from a lag time. It is not clear what a symmetric response would be for a third party (i.e., the one providing extended deterrence) on behalf of its supported partner. Should the United States jam or dazzle a Chinese satellite in response to Chinese actions against a Japanese system?

The situation is further complicated if the United States itself has not been targeted for cyber attacks. While one might try to draw a parallel with the nuclear deterrent situation of the Cold War, the difference in the two sides' political situations (i.e., the absence of Chinese allies) means that any response would be aimed directly at the PRC, inviting retaliation against the United States. There would be few "firebreaks" in terms of targets or effects. Consequently, a decision to engage in retaliatory cyber or space attacks to fulfill extended deterrence in the face of cyber or space attacks against an ally or friend would mean opening up the American information and space infrastructure to retaliation. (Again, this presumes that the attacker can in fact be identified with sufficient certainty to allow for American retaliation.)

The parallel further breaks down with regard to attribution of the response. While an American response in space to a space attack may have telltale characteristics that make clear it is an American response, the difficulties of attribution in cyberspace would extend to any American response. The United States may find it hard to signal its commitment to Japan if the PRC is subjected to a variety of attacks by a host of players, especially if there are third parties (e.g., non-threatened regional states who are nonetheless antagonistic to China) or non-governmental entities (e.g., citizen hackers, Anonymous) who are also engaging in cyber attacks.

Conversely, it may be that the combination of attribution and multiple players makes limiting escalation in the context of extended deterrence also more difficult. For the United States, there is the problem of determining a proportionate response to a cyber attack on an ally. What would be the proper counterpart to a cyber attack that damaged Japanese Self Defense Force command and control networks? Would shutting down the entire PLA conventional forces' C2 infrastructure (assuming it can be differentiated from its nuclear C2 structure) be proportionate or seen as opening the way for larger-scale American military strikes? This becomes much less problematic if the cyber and space attacks occur in the context of a larger military offensive, but that would return the focus to extended deterrence against conflict in general.

Extended deterrent responses in cyberspace also must address the dynamic nature of the cyber environment itself. In the first place, it is presumed that most cyber weapons can realistically only be used once; once exposed, the target is likely to take remedial actions that will negate any further attempts to exploit that particular weakness. It may be that some types of vulnerabilities may be harder to resolve than others (e.g., pervasive, hardware-based vulnerabilities would take longer to address simply because of physical constraints). Consequently, any decision to use a cyber weapon would effectively mean its removal from the inventory, making a decision to use such a tool on behalf of a partner a critical one.

Moreover, if one is seeking to respond to an adversary's initial cyber attack, it is likely that the adversary will have already moved to limit their own vulnerability (e.g., moving to air-gapped systems, initiating stricter security protocols, etc.). Consequently, one cannot be sure if the pre-conflict array of cyber weapons and tools would be available once the conflict has started, especially if the adversary initiates them. As important, simply in the course of day-to-day activities, software patches, security updates, etc., may eliminate or reduce vulnerabilities. The ability to credibly (i.e., consistently and effectively) engage in extended deterrence in the cyber domain is therefore always subject to an adversary's actions.

Chinese Perspective on Deterrence and the Space and Cyber Domains

Chinese views on deterrence, as noted earlier, differ significantly from Western views, beginning with the greater emphasis on coercion.[153] There is little evidence that the Chinese are focusing much effort on deterring actions in space or the cyber realm; instead, their writings suggest a much greater emphasis on coercing an adversary through actions in the space and cyber domains, often in conjunction with conventional and even nuclear forces.

Space Deterrence[154]

Space deterrence (*kongjian weishe*) is characterized by the PLA as the use of space forces and capabilities to deter or coerce an opponent, preventing the outbreak of conflict, or limiting its extent should conflict occur.[155] By displaying one's own space capabilities and demonstrating determination and will, the PLA would hope to induce doubt and fear in an opponent so that they would either abandon their goals or else limit the scale, intensity, and types of operations.

It is important to note that space deterrence is not aimed solely, or even necessarily, at deterring actions in space, but rather, in conjunction with nuclear, conventional, and informational deterrence capabilities and activities, at influencing an opponent's overall perceptions and activities. PLA teaching materials suggest that there is a perceived hierarchy of space deterrence actions, perhaps akin to an "escalation ladder" involving displays of space forces and weapons, military space exercises, deployment or augmentation of space forces, and employment of space weapons.

Displays of space forces and weapons (*kongjian liliang xianshi*) occur in peacetime or at the onset of a crisis. The goal is to warn an opponent in the hopes of dissuading them from escalating a crisis or pursuing courses of action that will lead to

---

[153] For a more extended discussion of Chinese views of deterrence, see Dean Cheng, "Chinese Views on Deterrence," *Joint Force Quarterly*, Issue 60 (First Quarter 2011), 92-94, http://www.dtic.mil/doctrine/jfq/jfq-60.pdf (accessed October 15, 2015).

[154] This section is drawn from Jiang Lianju, *Space Operations Teaching Materials* (Beijing: Military Science Publishing House, 2013), and Chang Xianqi, *Military Astronautics*, 2nd ed. (Beijing: National Defense Industries Press, 2005).

[155] Jiang Lianju, *Space Operations Teaching Materials*, 126.

conflict. Such displays involve the use of various forms of media to highlight one's space forces and are ideally complemented by political and diplomatic gestures and actions, such as inviting foreign military attachés to attend weapons tests and demonstrations.

Military space exercises (*kongjian junshi yanxi*) are undertaken as a crisis escalates if displays of space forces and weapons are insufficient to compel an opponent to alter course. They can involve actual forces or computer simulations and are intended to demonstrate one's capabilities but also military preparations and readiness. At the same time, such exercises will also improve one's military space force readiness. Examples include ballistic missile defense tests, anti-satellite unit tests, exercises demonstrating space strike (*kongjian tuji)* capabilities, and displays of real-time and near real-time information support from space systems.

Space force deployments (*kongjian liliang bushu*) are seen as a significant escalation of space deterrent efforts. They occur when one concludes that an opponent is engaged in preparations for war and involve the rapid adjustment of space force deployments. As with military space exercises, this measure is not only intended to deter an opponent, but also, should deterrence fail, is seen as improving one's own preparations for combat.

Such deployments, which may involve moving assets that are already in orbit and/or reinforcing current assets with additional platforms and systems, are intended to create local superiority of forces so that an opponent will clearly be in an inferior position. They may also involve the recall of certain space assets (e.g., space shuttles) either to preserve them from enemy action or to allow them to prepare for new missions. This may be akin to the evacuation of dependents from a region in crisis as a signal of imminent conflict.

The Chinese term the final step of space deterrence as "space shock and awe strikes" (*kongjian zhenshe daji*). If the three previous, less-violent deterrent measures are insufficient, then the PLA suggests engaging in punitive strikes so as to warn an opponent that one is prepared for full-blown, comprehensive conflict in defense of the nation. Such strikes are seen as the highest and final technique (*zuigao xingshi he zui hou shouduan*) in seeking to deter and dissuade an opponent. Employing a

combination of hard-kill and soft-kill methods, one would attack an opponent's physical space infrastructure and data links. If this succeeds, opposing decision-makers will be psychologically shaken and cease their activities. If it fails, an opponent's forces will nonetheless have suffered some damage and losses, which will help ensure victory in the course of open conflict.

Information Deterrence

According to PLA writings, "information deterrence" (*xinxi weishe*) conceptually includes deterrence in the cyber realm but goes further, encompassing all aspects of information and information operations. It is defined in the PLA's terminological reference volume as "a type of information operations activity in which one compels the adversary to abandon their resistance or reduce the level of resistance, through the display of information advantage or the expression of deterrent/coercive information."[156]

The 2007 edition of the PLA Military Encyclopedia defines "information deterrence" as those activities in which "threats that employ information weapons or which implement information attacks against an opponent, lead to shock and awe and constrain the adversary."[157] Another Chinese study guide defines it as "a national display of information advantage or the ability to employ information operations to paralyze an adversary's information systems, so as to threaten that adversary. This serves to constrain the other side, as part of the deterrent/coercive goal."[158]

What is clear across these various definitions is that "information deterrence," like the broader Chinese conception of deterrence in general, includes both dissuasion and coercion and embodies the idea of deterring through information operations rather than deterring operations in information space.

---

[156] *Chinese People's Liberation Army Terminology* (Beijing: Military Science Publishing House, 2011), 262.

[157] Chinese People's Liberation Army, National Defense University Scientific Research Department, *Chinese Military Encyclopedia,* 2nd ed., *Military Strategy* (Beijing: Chinese Encyclopedia Publishing House, 2007), 283.

[158] AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide – 100 Questions About Informationized Operations* (Beijing: Military Science Publishing House, 2005), 15.

Information deterrence, as with all the various Chinese concepts of information warfare, is built upon the ability to establish "information dominance" (*zhi xinxi quan*), the ability to control information within a given time and region, including one's own ability to obtain and exploit information, and denying the adversary that same ability.[159] Information deterrence, however, is more focused on influencing those who use information than on affecting the flow and exploitation of information, except insofar as the latter supports the former.

Information deterrence is largely tied to information offensive operations (*xinxi jingong zuozhan*), and especially network offensive operations (*wangluo gongji li*). Because they require little overhead and have multiple means of being implemented, information offensive operations are hard to defend against. Network offensive operations have the added advantage that the attacker has the advantage of the initiative.

Information deterrence is important in peacetime because it can help manage crises and limit the potential for the outbreak of war. Such operations have the added advantage over conventional or nuclear deterrence because they are more credible, since information offensive operations can be undertaken in peacetime without precipitating conflict.[160] They are important in the event of crisis because they can affect every aspect of an adversary's decision-making process while also strengthening one's own overall military situation.

Thus, not only will an adversary be influenced directly by information offensive operations, but the improvements in the relative balance between oneself and the adversary will reinforce the deterrent and coercive effects.

The use and threatened use of information warfare capabilities (including weapons and methods) are seen as an integral part of information deterrence efforts. In particular, by demonstrating to an opponent the ability to erode or deny information access, PLA analysts believe that this would jeopardize an opponent's overall ability to conduct the joint operations essential to informationized warfare. "It

---

[159] Chinese People's Liberation Army, *Chinese Military Encyclopedia,* 2nd ed., *Military Strategy*, 213.

[160] Chi Yajun and Xiao Yunhua, *Essentials of Informationized Warfare and Information Operations Theory* (Beijing: Military Science Publishing House, 2006), 252.

may be said that in joint campaigns, without information dominance, one cannot sustain comprehensive battlefield dominance."[161] The inability to conduct joint operations, in turn, would mean that an adversary would be operating at an enormous disadvantage and would likely concede or at least defer conflict.

The relationship between information dominance and space dominance is seen as especially intimate, for without reliable access to information on a timely basis, one cannot ensure that space weapons and information systems can safely operate or be controlled and used effectively in combat. "Therefore, without battlefield information dominance, there can be no battlefield space dominance."[162]

Information deterrence is also closely tied to the psychological warfare aspect of information warfare. Local wars under informationized conditions already impose a significant psychological cost. Cognitive and emotional processes are often subject to serious interference and stress, given the more intense nature of such conflicts. The will of both top military and civilian leaders as well as the broader population will also be under much greater pressures from deliberate psychological warfare, as well as threats of attacks from various quarters (including network and electronic warfare).[163]

Particularly powerful tools for psychological warfare in support of information deterrence are the media (especially television) and the Internet, coupled with specifically provided information. News media, especially television news, is seen as having both a broad audience and a broad acceptance and authoritativeness, allowing it to generate broad reactions. Similarly, the Internet not only has permeated many societies, but is virtually impossible to control, so that messages aimed at eroding support are difficult to muzzle.

Implications for Extended Deterrence in the Asia–Pacific

Interestingly, some Chinese analysts seem to believe that a state of mutual "information deterrence" already exists in the Asia–Pacific region, at least insofar as disruptive attacks against each other's information networks are concerned. It is noted

[161] Li Yousheng, *Joint Campaign Teaching Materials* (Beijing: Military Science Publishing House, 2012), 69.
[162] Ibid., 70.
[163] Chi Yajun and Xiao Yunhua, *Essentials of Informationized Warfare and Information Operations Theory*, 302-304.

that among states of roughly equal levels of information technology, and given the wide penetration of the Internet into all aspects of all nations' societies, economies, and political structures, states will not engage in disruptive network warfare lightly.[164] This would suggest that with respect to computer network exploitation (i.e., cyber espionage), there is some degree of restraint against proceeding to erase data or physically destroy key elements of a potential adversary's information networks, at least in peacetime.

More worrisome, some Chinese writings suggest that in time of crisis, one needs to remind an adversary of one's ability to plant viruses or otherwise undertake information attacks (*xinxi jingong*) in order to warn them to cease their policies or otherwise coerce them. At a minimum, such moves are seen as promoting psychological pressures, as they will arouse fear and may undermine will.[165]

If there is a basic symmetry of perspective and capability in information capabilities on the two sides of the Pacific leading to a broad form of mutual direct deterrence, the same is not true for extended deterrence. The diverging political context for extended deterrence in the Asia–Pacific in the 21st century, compared with that in Europe during the Cold War, coupled with the different perspectives on extended deterrence in the space and cyber realms, has important implications for the United States.

Most importantly, the PRC is not focused on engaging in extended deterrence (given the lack of an alliance network), but on *countering* extended deterrence. In particular, the PRC sees itself at present as likely confronting the United States should it be compelled to consider the use of force against Taiwan or Japan. It therefore sees cyber and space *weishe* activities as seeking to coerce Taiwan and Japan to accommodate Chinese demands while ideally dissuading the United States from acting.

But such actions are unlikely to occur independently of larger efforts at both coercion and dissuasion. That is, it is unlikely that the PRC would rely only on space

---

[164] AMS Operations Theory and Regulations Research Department and Informationized Operations Theory Research Office, *Informationized Operations Theory Study Guide*, 15.
[165] Chinese People's Liberation Army, National Defense University Scientific Research Department, *Chinese Military Encyclopedia,* 2nd ed., *Military Strategy*, 283.

or cyber actions to message their intentions (although there may be only space or cyber activities at any given moment). As important, there is no evidence that the Chinese would be intent on deterring actions in space and/or cyber whether in a crisis or day-to-day, whether in a basic or extended deterrence framework.

For the United States, then, the issue in the Pacific does not really differentiate between basic deterrence and extended deterrence, and outer space and the cyber environment are only additional areas where signaling can occur. Beijing will look to American actions in the aggregate, including naval movements and air and ground force deployments, as well as activities in outer space and the cyber environment in assessing American commitments—the essence of "extended deterrence." At the same time, it will also employ its own air, land, sea, space, and cyber forces to signal its own resolve and intentions.

About the Authors

Gordon G. Chang is the author of *The Coming Collapse of China* and *Nuclear Showdown: North Korea Takes on the World*. He is a columnist at *The Daily Beast* and a *Forbes.com* contributor, and he blogs at *World Affairs Journal*. His writings on China and North Korea have appeared in the *New York Times*, the *Wall Street Journal*, the *International Herald Tribune*, *Commentary*, *Weekly Standard*, *National Review*, *National Interest*, and *Barron's*.

Dean Cheng is the Heritage Foundation's Senior Research Fellow on Chinese political and security affairs. He specializes in China's military and foreign policy, specifically its relationship with the rest of Asia and the U.S. He has testified before Congress, and has been interviewed by or provided commentary for publications such as *Time Magazine*, the *Washington Post*, *Financial Times*, *Bloomberg News*, *Jane's Defense Weekly*, South Korea's *Chosun Ilbo and*, and Hong Kong's *South China Morning Post*.

Frederick Fleitz is Senior Vice President for Policy and Programs at the Center for Security Policy. He held U.S. government national security positions for 25 years with the CIA, DIA, the Department of State and the House Intelligence Committee staff. His articles on international security topics have appeared in the *Wall Street Journal*, the *Jerusalem Post*, the *New York Post*, *National Review*, *Investor's Business Daily*, and the *International Journal of Intelligence and Counterintelligence*.

Kevin D. Freeman, CFA, is founder of Freeman Global Holdings, LLC, a specialty consulting firm which shares Freeman's unique understanding of the global capital markets and their intersection with national security issues. He is considered one of the world's leading experts on economic warfare and financial terrorism, having briefed members of the U.S. House, Senate (present and past), CIA, DIA, FBI, SEC, Homeland Security, the Justice Department, as well as local and state law enforcement agencies.

Frank Gaffney is the founder and President of the Center for Security Policy. Under Gaffney's leadership, the Center has been nationally and internationally recognized as a reputable resource for foreign and defense policy matters. Mr. Gaffney was the Deputy Assistant Security of Defense for Nuclear Forces and Arms Control Policy from 1983 to 1987. Following that he was nominated by President Reagan to become the Assistant Secretary of Defense for International Security Policy.

Bill Gertz is senior editor of the *Washington Free Beacon*, and national security columnist at the *Washington Times*. Bill is the author of six books, four of which were national bestsellers. The Chinese state-run *Xinhua* news agency in 2006 identified Gertz as the No. 1 "anti-China expert" in the world. Gertz insists he is very much pro-China-pro-Chinese people and opposed to the communist system.

Admiral James "Ace" Lyons, Jr., USN (ret), is President/CEO of LION Associates LLC, a premier global consultancy providing technical expertise. As an Officer of the U.S. Navy for thirty-six years, most recently as Commander in Chief of the U.S. Pacific Fleet, his initiatives contributed directly to the economic stability and humanitarian understanding in the Pacific and Indian Ocean regions and brought the U.S. Navy Fleet back to China.

Peter Navarro's latest bestselling book *Crouching Tiger: What China's Militarism Means for the World* is rated as one of the Top Ten Books of the Year by *The Globalist*. Peter Navarro is a distinguished keynote speaker and holds a Ph.D. in economics from Harvard University. He has been a business professor at the University of California-Irvine for more than 20 years, where he was awarded the Distinguished Faculty Award for Teaching on the UCI campus in 2015.

Lindsey Neas previously served as a U.S. Army officer. He was chief of staff of the Graham-Talent WMD Commission ('09-'10) and for 15 years served as a defense aide to Senator Talent and several other members of the Senate and House Armed Services Committees.

Senator James Talent is a senior fellow and the director of the Marilyn Ware Center for Security Studies' National Security 2020 Project at the

American Enterprise Institute. He has been active in public policy for the past 30 years, including representing Missouri in both the US Senate and House of Representatives. While serving in the Senate, he was a member of the Senate Armed Services Committee and chairman of the Subcommittee on Sea Power for four years.