STRATEGIC STUDIES QUARTERLY

China's Competitive Strategy: An Interview with Robert O. Work

Conducted 10 October 2018

This interview is an outgrowth from Secretary Work's 2018 Center for a New American Security annual conference presentation detailing the five-step Chinese competitive strategy against the United States. China's strategy is designed to overcome technological inferiority, move to technological parity, and achieve technological superiority.

SSQ: The first step you mention in China's strategy is industrial and technical espionage (ITE). Did the United States miss or simply ignore this threat?

ROW: We have become increasingly aware of the nature of the threat, which is unlike any we have faced before. During the Cold War, espionage was more about turning agents and getting intelligence agents to turn over documents and reveal adversary agents. However, in the case of China, it is more a cyber-intellectual property threat—getting into systems and exfiltrating data. We were therefore unprepared for the Chinese approach—especially on the industrial wide-scale the Chinese use. Consequently, our response lagged.

Lately, we have been successful in implementing different types of measures to counter their strategy, but the Chinese still pursue industrial espionage in a very big way. Let me give you an example of why this is important. Frank Kendall, the former Office of the Secretary of Defense acquisition executive, did a study and found that once the United States or the Chinese decides to build a new fighter, the time spent in development and production engineering was roughly equal. However, through intellectual property theft and data exfiltration, the Chinese are able to reduce significantly the time spent doing research and prototype engineering. This is why they have been able to field capabilities consistently quicker than we expected. From a historical perspective, the Chinese have been making a concerted effort to acquire US technological capabilities since the late 1990s. What they have been able to accomplish in the past 20 years is quite remarkable.

01-Work 2019-01.indd 2 1/22/2019 7:57:56 AM

SSQ: Are we as a nation better at preventing ITE now or do we remain vulnerable?

ROW: We remain vulnerable, but we are much more attuned to the threat. As a result, the US has hardened its networks and its supply chain. In addition, all of our contractors have become much more aware and are hardening their networks. Furthermore, while they may not be able to stop a determined intrusion, they are much more successful in halting data exfiltration. I would not want to declare victory against the threat, however, the US is in a much safer position today than we were three or four years ago.

SSQ: You list *system destruction warfare* as the second aspect of their strategy, which is focused on achieving a decisive advantage in information superiority. Do you see this as feasible today given the complexity and redundancy of the US system?

ROW: Yes, it is certainly feasible if we don't take the threat seriously and prepare to defeat it. System destruction warfare is central to the Chinese theory of victory in high-technology, "informationalized" warfare. This type of warfare sees collisions between what we refer to as *operational battle networks*—what the Russians call *reconnaissance-strike complexes*, and the Chinese refer to as *operational systems*. System destruction warfare concentrates on disabling the sensor, command and control, and effects grids common to all battle networks. If Chinese efforts are successful, they will be able to prevail in a guided munitions salvo competition and gain an enormous advantage at the operational level of war.

So, Chinese planners expend a large amount of time and effort thinking about how to destroy our battle networks. Every single one of our network nodes and links are covered by some type of Chinese electronic warfare capability, including all our radars and sensors. We suspect the Chinese have also developed cyberweapons to attack the Department of Defense (DOD) internet of things (IoT). They have long-range anti-aircraft missiles that can shoot down our Airborne Warning and Control System (AWACS) and Joint Surveillance and Attack Radar System (JSTARS) type aircraft. When surveying all of their capabilities, the Chinese have quite a broad, very well-developed strategy.

If the US ever gets into a fight with the Chinese, we had best be prepared to "weather the storm" and fight through Chinese efforts to cripple

01-Work 2019-01.indd 3 1/22/2019 7:57:56 AM

our sensor, command and control, and effects grids. The outcome of the fight will likely be determined by our success in doing so.

SSQ: Where are we most vulnerable and where are the Chinese most vulnerable?

ROW: A great source of information on this subject is the recent Government Accounting Office (GAO) report, titled *Weapons System Cybersecurity.* It focuses on the vulnerability of the DOD IoT, which is probably our greatest cyber vulnerability right now. DOD systems and platforms have all types of attack surfaces through their apertures and control systems, and the services do not spend enough time addressing these vulnerabilities. Doing so is neither glamorous nor inexpensive. Given a choice, most of the services prefer to buy new platforms rather than try to "cyber harden" old platforms. However, as the GAO report states, even the new platforms are not all that cyber resilient. DOD has spent much money over the past five years to harden our networks, and while we remain vulnerable, we are far less so than before. Over the same period, however, we have not spent nearly enough on hardening the DOD IoT. As a result, I believe GAO is right when they say that DOD is just beginning to grapple with the scale of its IoT vulnerabilities. We have a long way to go in this regard.

As for Chinese vulnerabilities, it is difficult for me to answer because this information is classified, and I have not seen recent net assessments. However, in general, their operational systems have the same vulnerabilities as our own battle networks; their sensor, command and control, and effects grids, as well as their IoT, are all vulnerable to intrusion and attack. We also spend much time identifying and planning to exploit these vulnerabilities. However, I cannot say if they are more or less vulnerable than we are.

SSQ: *Firing effectively first* is another part of China's competitive strategy. How would you assess their capabilities to execute a preemptive first strike today and in the next five years?

ROW: The Chinese have focused on being able to fire effectively first, a key principle of guided munitions warfare. Since guided munitions warfare is an offensive dominant regime, the side that gains an early advantage in attacking the adversary's battle networks, command and control nodes, and high-value targets starts to accrue advantages right

01-Work 2019-01.indd 4 1/22/2019 7:57:56 AM

away, and these compound over time. So there are very high incentives for preemption.

However, Chinese thinking goes well beyond preemptive attacks. They consistently try to build weapons that "out stick"—that is to say, out-range—US weapons. Where successful, Chinese forces will be able to concentrate fire on portions of US forces before the US can bring their own weapons to bear. They also pursue weapons designed to penetrate US defenses with high probabilities of success. For both these reasons, the Chinese have adopted ballistic missiles as their primary kinetic effectors.

Chinese military planners assessed how the US employed airpower during Desert Storm and decided not to try and compete symmetrically—at least initially. Instead, they pursued a world-class ballistic missile force, which is far easier to build, train, and maintain than a world-class air force. And there are other advantages: it is generally easier to extend the range of ballistic missiles than it is to extend the unrefueled range of land-based aircraft. Additionally, ballistic missiles are difficult to shoot down and impose a high burden on US defenses. Moreover, it is easier to plan and prepare a large missile strike with little or no warning than it is for a comparable air force. Preparations for a major air operation would create all sorts of indications of warnings, including aircraft marshaling, munitions buildup, fuel stockpiles, and training. However, a missile force can deploy to their launch points and execute strikes with relatively little notice, especially under cover of a preplanned exercise.

Chinese doctrine thus emphasizes long-range missile warfare and high-density salvos. The Chinese have air-to-air missiles that outrange our own. They have long-range ballistic missiles, sea-based ballistic missiles, and anti-ship cruise missiles with greater ranges than our own. In every case, the Chinese will try to "out stick" us and overwhelm our defenses by using mass salvos. This is part of their strategy and doctrine of firing first effectively.

SSQ: Do you expect the United States and our allies will have indications and warnings of a preemptive strike?

ROW: Generally speaking, if the Chinese decide to fight the United States, I would expect them to launch concentrated surprise attacks against Joint forces in theater. On the other hand, even in times of heightened tensions, it is hard for me to imagine the US launching a surprise preemptive strike against Chinese forces. As a result, US forces

01-Work 2019-01.indd 5 1/22/2019 7:57:56 AM

will likely have to take the first punch. This presents the US with a tough asymmetrical disadvantage. Regardless of whether we have the benefit of warning or not, I think we need to accept that in a war with China, the Chinese would likely fire the first salvo to try and preempt us rather than us trying to preempt them. Consequently, US forces must be prepared to survive a surprise preemptive attack and shift immediately to the offensive. This places a high burden on our forces regarding training and preparedness.

SSQ: You listed *secret capabilities* as the fourth step in the strategy that allows China to reveal capabilities to deter and conceal them to win. Is the United States at a great disadvantage in capabilities or is this simply a great unknown?

ROW: We have a lot of so-called "black capabilities" protected by special compartmented information and special access programs. We must assume the Chinese do, too. And the fact of the matter is, we will only know for certain if we are at a disadvantage if we find ourselves in a fight with the Chinese.

This is an important point. In any long-term military-technical competition, competitors will reveal some capabilities to deter their opponents and will conceal certain capabilities in hopes of gaining a potential war-fighting advantage in the early stages of war. Deciding what capabilities to reveal and what capabilities to conceal is a key part of any competitive strategy. For example, when people think back to the second offset strategy, some say it was all about long-range sensors, precision-guided munitions, and stealth. However, at the time we only revealed our ability to target and fire long-range conventional guided munitions. We did this to deter a Soviet invasion of Europe, and history suggests it helped to do just that. On the other hand, despite much speculation, we never revealed stealth technology until 1989. We opted to conceal our true stealth capabilities for war-fighting advantage should a Soviet attack come.

We must assume the Chinese are following the same playbook. Indeed, they refer to a special category of weapons termed *assassin's mace* in the belief these weapons will be decisive in a conflict with the US. They have opted to reveal some of these capabilities. For instance, they've demonstrated the DF-21 "carrier killer," a ballistic anti-ship missile with a range of over 800 miles. They also demonstrated the ability to threaten

01-Work 2019-01.indd 6 1/22/2019 7:57:56 AM

US satellites with a direct ascent anti-satellite interceptor. Most recently, they've demonstrated a variety of hypersonic weapons. Presumably, they are demonstrating these capabilities to deter any US intervention against them. At the same time, however, President Xi has instructed the Chinese military to conceal "the sharpest weapons of the state." So, despite our best efforts to track and understand Chinese capabilities, we must be prepared for technological surprises on the first day of a war that we hope will never come. Under these circumstances, we must be able to shake off the surprise, quickly develop countermeasures against them, and continue to fight.

Furthermore, let me offer an observation about high-tech weapons. For example, when you look back at Vietnam, the AIM-7 Sidewinder and the AIM-9 Sparrow air-to-air missiles were not nearly as effective in combat as we expected them to be; their observed probability of a kill turned out to be far less than we anticipated. We can anticipate the same thing in a future war between high-technology adversaries. For both sides, some of the weapons will perform better than expected, others will perform worse than expected, and both sides will be confronted by weapons they did not expect. In this high-tech competition, we cannot assume we will always have the advantage and must anticipate a high degree of technological surprise. The force better able to shrug off surprise and continue to operate effectively will likely be the winner.

SSQ: The final area of China's strategy is to *exploit artificial intelligence* (AI) for military superiority and lead in this area by 2030. Can you compare and contrast US-China AI progress to date? Who is leading and where?

ROW: We know the Chinese have a national plan that seeks to catch up with the United States in AI technologies by 2020. I think they've done that already, having achieved broad parity in computer vision, machine learning, and natural language processing. Their next goal is to vault ahead of the Americans not later than 2025 by concentrating on fielding AI applications. For example, in terms of military applications, how might AI improve their missile guidance and performance? What are the most effective applications for vehicles? For decision-making systems? By 2030, the Chinese want to be recognized and unchallenged as the world leader in AI technologies. They believe this is one way to surpass the US as the world's leading military power.

01-Work 2019-01.indd 7 1/22/2019 7:57:56 AM

Right now, it is difficult to say who might be ahead of the US as it begins to marshal its resources in response to the Chinese plan. So, the answer is unclear, and frankly, it might not become clear until we get into a conflict. This competition is not like the Cold War when satellites could overfly a country and observe and count forces. During that time—from what we could see—we could assess and predict their combat potential. Today, AI technologies are hidden within command and control and weapons systems, and their full capabilities will not be revealed until the first time they are used. So once again, we need to be prepared for a surprise. This is why when approaching this competition we need to remember the advice of all politicians: always assume you are losing the race.

SSQ: A recent Brookings survey showed mixed approval for integrating AI with military capabilities. Do you have any concerns or fears about doing this?

ROW: To understand this question, you must understand the difference between two types of AI: narrow AI and general AI. Narrow AI is the programmed ability of a machine to create its own courses of action and to choose among them to perform an assigned task. Think for instance, about the parallel parking application in your car. You pull your car abeam the spot, the computer prepares a thousand calculations or courses of action, and it chooses one. It signals you, "I've chosen an option, now pull your car forward three feet and stop." The computer then takes over and executes the task. This is narrow AI. The computer is programmed to perform only a limited function, in this case, parallel parking, not speeding off to Jiffy Mart. We want to inject a wide range of narrow AI applications in US sensor, command and control, and effects grids. By doing so, we think we will be able to make faster and more relevant decisions and apply effects more rapidly and discretely.

By contrast, general AI is the programmed ability of a machine to set its own goals, learn from them, and change them. People are most worried about general AI in a freewheeling machine that can set its own goals more like Skynet and the Terminator. DOD has the very same worry. That is why it has stated it will always seek to have a human in the loop when making a lethal decision on the battlefield.

So, to reiterate, I think that people who are worried about putting AI in weapons are really objecting to the use of general AI. They should,

01-Work 2019-01.indd 8 1/22/2019 7:57:56 AM

therefore, be happy to know that DOD neither wants general AI weapons nor is pursuing them. No commander would want an AI weapon deciding what to attack on a given day, and then deciding to change the target. Commanders will much prefer assigning a target to a narrow AI weapon, and letting the weapon decide the best way to attack it. This is similar to other "fire and forget" weapons currently in use. While we need much more debate on this issue, the current debate is being hampered by the lack of common understanding of the actual argument.

***SSQ*:** A recent Geneva meeting of experts began discussions on forming international norms and laws for AI. What are your views on the prospects for success of such norms?

ROW: It is very difficult to envision how international norms on AI could be enforced. There might be some basic international norms that should be created, particularly concerning general AI, but I am skeptical even these basic norms would be feasible. The reason I feel this way is that the march toward smarter decision aids and smarter weapons powered by machine intelligence cannot be stopped and the true capabilities of these technologies will be hidden until they are employed. There may well be certain applications the international community desires to prohibit, but again, I am skeptical any of these could be enforced.

SSQ: In your presentation, you assert that China's competitive strategy is eroding conventional deterrence. How do you see deterrence failure emerging and why?

ROW: It could emerge as a consequence of China's emphasis on firing effectively first. Since guided munitions warfare is offensive dominant, should the Chinese opt for war, incentives for preemption are extremely high. That makes crisis instability more acute. Another issue many people are uncertain of and worry about is, if we rely too much on machines for indications and warning, the machines might make a mistake and therefore undermine deterrence. Now, this is not much different from the problems we had in the past where humans had to interpret a wide variety of different information to decide whether an attack was occurring. However, many people are worried about such a machine-driven scenario and are working through the implications. We do not have all the answers yet.

01-Work 2019-01.indd 9 1/22/2019 7:57:56 AM

SSQ: Given that China is unlikely to change its strategy, how should the United States challenge each of these five aspects? What must we do now and in the future?

ROW: There are many things we could and need to do. The first step is to fight back against Chinese industrial and technological espionage and make sure we are meeting this threat head-on. We must take concrete actions to deter the Chinese from continuing these efforts.

In responding to Chinese emphasis on system destruction warfare, we have a lot more to do. In the 1980s, we had a revolution in training where we implemented the *opposition force* concept. The Army started training at the National Training Center, the Air Force had Red Flag, and the Navy had Top Gun. Today, we need an opposing force that is proficient in all aspects of system destruction warfare. Every time we have an exercise, this force should try to take down our networks. This will be the best way to improve our operations and make our systems and tactics, techniques and procedures, more resilient. We must be better at this game than the Chinese! Our force structure must also begin a broad shift toward more survivable platforms. In my opinion, the JSTARS cancellation is the first indicator that we are serious about moving forward. We should be doing the same thing with AWACS. Both of these systems will likely be replaced by a combination of distributed manned and unmanned systems and platforms with high degrees of narrow AI. Also, we must introduce additional and better "cognitive" tactical electronic warfare and cyber capabilities at the forward line of troops like the Army is now planning to do.

The US can do many things to address China's strategy of firing effectively first. In addition to destroying China's operational systems to avoid being targeted, we can introduce more long-range weapons and more counterforce weapons of our own. In this regard, the Navy is modifying its Tomahawk missile to allow it to attack ships. The Air Force is extending the range of its stealthy JASSM missile. And the defense department is aggressively pursuing long-range hypersonic weapons.

We must continue to reveal capabilities we think will deter the Chinese. At the same time, we should conceal things we think will provide a war-fighting advantage if and when a conflict begins. We have to also train our force for technological surprise while at the same time being adaptive to it.

01-Work 2019-01.indd 10 1/22/2019 7:57:56 AM

Finally, on the AI front, we have to compete as a nation, not just as DOD. This is a national competition that will determine our economic and military competitiveness in the twenty-first century. We must respond to the China challenge by marshaling our national capabilities and competing vigorously.

And let me end with this thought. China is, without question, going to be the most difficult competitor the US has ever faced. However, it is important to note that neither the national security nor national de-fense strategies refer to China as an adversary or an enemy. Instead, they refer to China either as a geopolitical rival or a strategic competitor. This choice of words signals we don't believe a war with China is inevitable. However, both strategies make clear we are in a long-term strategic com-petition where the Chinese aim to surpass the US as the number one economic and military power in the world. The United States faces a choice: either respond to this challenge or succumb to it. Should we choose to confront the challenge, the US *must* take steps to remain com-petitive and become even more competitive.

SSQ: Secretary Work, on behalf of team SSQ and our SSQ audience, allow me to thank you for sharing your ideas on what may well be the greatest challenge to US national security in the twenty-first century. SSQ

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.

01-Work 2019-01.indd 11 1/22/2019 7:57:56 AM