AUGUST 2023

Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario

By James A. Lewis

Expressions of surprise that the Chinese military **targeted** critical infrastructure in Guam for cyber reconnaissance are misleading. Of course the People's Liberation Army (PLA) is conducting cyber reconnaissance; China has been probing U.S. critical infrastructure networks for vulnerabilities since the Obama administration, if not before. From a military perspective, this is the kind of reconnaissance any capable nation would engage in against a potential opponent to identify targets and possibly prepare them for cyberattack. What was misleading in these reports is that critical infrastructure in Guam was not the primary target. The primary targets, particularly those that would support U.S. forces in any engagement over Taiwan, are located in the United States. China is engaged in a major cyber reconnaissance effort against them. If China is willing to accept the risk of broadening a conflict over Taiwan, it may decide that cyber actions against civilian infrastructure in the United States could usefully disrupt communications and the flow of material needed for military operations.

Chinese decisionmaking on the use of offensive cyber operations against civilian critical infrastructure will be shaped less by the likelihood of detection and attribution and more by a desire to manage escalation and retaliation. China may decide not to use wide-scale cyber disruption and reserve its efforts for espionage. A decision on how and where to use cyberattacks will also be shaped by the progress (or lack thereof) in any Chinese offense; a lack of success could lead to more aggressive cyber actions. The broad calculus for China's decisionmaking will likely involve weighing the relative military advantage gained from cyberattacks on critical infrastructure against the probability that such attacks would provoke a harsh U.S. response or expand the conflict.

Some of China's decisions will be shaped by resource constraints. Cyberattacks are often tailored for specific vulnerabilities and targets have a greater chance of success but take time (usually a few months) to develop. Even China faces limits on skilled personnel. These two factors suggest some prioritization of targets for cyberattack. A Chinese priority list of targets will be shaped by a balance between the likely military payoff and the political risk of expanded conflict.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

This estimate assumes that China does not engage in reconnaissance of targets unless it is considering attacking them. It is also based on Russian and U.S. practice in using offensive cyber actions against opponents' critical infrastructures during invasion. China's **Strategic Support Force**, created in 2015, combines space, cyber, electronic, and information operation capabilities. Published Chinese military doctrines discuss the central role of informatized warfare, the importance of the cyber domain in any conflict between the United States and China, and strategies to achieve "**dominance** in the space, cyber, electromagnetic, and possibly psychological domains." The intent is to disrupt, paralyze, or destroy an opponent's operational capabilities. This makes it likely that China has considered attacks on critical U.S. civilian infrastructure.

> *The broad calculus for China's decisionmaking will likely involve weighing the relative military advantage gained from cyberattacks on critical infrastructure against the probability that such attacks would provoke a harsh U.S. response or expand the conflict.*

The most probable targets fall into three categories: The first would be electrical power facilities. The second would be the pipelines and railroads in the continental United States that connect to these locations. The third would be the logistics and communications networks, including those that support supply chains for manufacturing precision-guided munitions and military aircraft. Primary targets would include telecommunications systems in cities and regions where naval and air bases are located, such as California, Hawaii, and Washington State. All are logical targets for cyber disruption, and many are located on the United States' Pacific Rim. Disruptions at such targets would provide near-term, tangible military advantage and would be conducted in parallel with Chinese cyber actions against military targets, such as information systems and advanced weapons.

China's planning is likely bound by a desire to minimize the probability of a general war with the United States. Cyberattacks against targets in the continental United States and Hawaii could threaten to prolong any conflict and make it unmanageable. The question for China's leaders is whether quick and precise strikes on civilian critical infrastructure with temporary effects justify this strategic risk. In preparing to defend against cyberattacks, however, the United States cannot assume that China will decide on a minimalist course.

Likely Targets

All digital targets are vulnerable to some degree. Pipelines, for example, stretch for thousands of miles across several states and traverse sparsely populated areas. They are digitally controlled, with many possible points for both cyber and physical disruption. The ransomware attack on Colonial Pipeline showed that short-term disruption can produce political benefits. Although the Biden administration (led by the Transportation Security Administration) is taking steps to reduce risks, there are many possible digital and physical targets along the length of a pipeline, and hardening them will take time. Electric grids have always been considered high-value targets and the potential vulnerabilities of electrical grids are well-known. There has been progress in reducing vulnerability in the years since the 2007 Aurora test showed how a cyberattack could cause physical damage to an electrical power

generator, but electrical power generation and transmission remains perhaps the most valuable target for disruption by China.

China could also target the communications infrastructure for disruption. Ukraine's telecommunications infrastructure was a key target for Russia. In a Taiwan scenario, this could include attacks on undersea fiber-optic cables and communications satellites. It could also include kinetic attacks on physical infrastructure. Like pipelines, undersea fiber-optic cables stretch thousands of miles. They are most vulnerable in relatively shallow waters. Something as simple as a fishing trawler hooking and breaking a cable is effective. It is also likely that China will attempt to disrupt, blind, or disable both military and commercial satellites for reconnaissance, navigation, and communications. China may not distinguish between military and commercial satellites, and commercial satellites play an essential role in U.S. military communications. Chinese officials have privately complained about Starlink. China has practiced jamming and spoofing satellite signals for navigation, and media reports and leaked U.S. documents state that China has developed cyber "weapons" for use against U.S. satellites. Using cyber methods against satellites is less intrusive and less escalatory than kinetic attacks (though these cannot be ruled out) but may also have a lower probability of success.

The Ukraine war points to the vulnerabilities of the precision-guided munitions (PGM) supply chain and the importance of steady resupply. These are complex munitions, so delays in obtaining even a single part can slow or stop production. The experience of European allies in the 2012 air campaign against Libya, where they depleted their PGM stocks within a few days, is suggestive of the benefits of disrupting the PGM supply chain. The United States (and regional allies) can prepare for this by stockpiling PGMs, but Ukraine shows that consumption rates are higher than expected. A combined cyberattack could disrupt PGM production and resupply. However, it remains an open question as to whether disruption to PGM resupply would provide the near-term benefits most useful to China, since the damage could take weeks to appear.

Cyberattacks on other critical infrastructures are possible but offer less of a benefit to China. Disrupting financial networks may provide secondary benefits if credit cards won't work and cash is unavailable. Disrupting municipal traffic control systems would provide temporary (and easily remedied) disturbances. Civil air traffic management systems are likely targets since civilian air freight will play a role in the resupply of high-value equipment (like PGMs), but the effects of a cyberattack on air traffic control could be quickly remedied, given U.S. experience in dealing with air traffic disruptions. Attacks on other infrastructures are unlikely to provide any military or strategic benefit. Water supply in key metropolitan areas may be one exception to this, since telecommunications and electricity depend on it. In all instances, deciding on targets, their location, and whether to strike them using cyberattacks will require a careful calculation of immediate military benefit weighed against the strategic risk.

Factors Affecting Chinese Decisions to Use Cyberattacks

Before Ukraine, given U.S. military setbacks in the Middle East and Xi Jinping's belief that the West was in irreversible decline, the Chinese government likely overestimated the level of action they could engage in without risk. The Western response to Ukraine, including sanctions against Russia and financial and military support for Ukraine, has led China to recalculate the costs of action against Taiwan, but domestic political pressures could still impel Xi to act.

Although it is currently unlikely that China will use force to occupy Taiwan, if it does decide to do so, it would undoubtedly prefer a short, sharp conflict, sinking a few U.S. carriers while holding off any U.S. response until its forces occupied the country. The PLA has, after all, been practicing some kind of Taiwan invasion scenario for 70 years. Their calculations may be similar to those made by Axis forces before World War II: that a sharp, decisive blow against U.S. naval and air forces in the Pacific region at the onset of conflict would stop the United States from intervening and dissuade it from continuing the conflict.

Factors that shape the calculations that apply to critical infrastructure are the comparative risks of striking civilian versus military targets, and the risk of striking targets in the continental United States. If China chose to attack civilian infrastructure in the continental United States, the most effective cyber actions against critical infrastructure would unavoidably affect several large U.S. cities, such as San Diego, Los Angeles, Seattle, and Honolulu. Collateral damage is inevitable if electrical power, telecommunications, and fuel pipelines are attacked. These are civilian infrastructures, but they are legitimate targets. The United States has attacked similar targets in the past, showing restraint when it believed it would quickly occupy opponent territory and need these infrastructures for itself. China does not face similar constraints, and the risk of civilian casualties from cyberattack in these cities is extremely low—the intended result is most likely the disruption of critical infrastructure, not physical damage or casualties.

China may consider targeting Washington, D.C., in the hope that disruption to power and communications in the nation's capital would slow any U.S. response; however, the degree of resilience found in national command systems and the risk of a fierce U.S. response to a cyberattack on the capital suggest that Chinese efforts at disruption in D.C. are unlikely. It is also likely that China would prefer to reserve cyber tools for intelligence gathering rather than disruption since it has had a long record of remarkable successes against the U.S. government.

> *It is also likely that China would prefer to reserve cyber tools for intelligence gathering rather than disruption since it has had a long record of remarkable successes against the U.S. government.*

Chinese planners face the complications of having to consider attacks on U.S. military facilities located in allied territory, particularly Japan. If Japan has not entered the conflict, it would be in China's interest not to attack targets in Okinawa or other areas. If Japan has entered the conflict, China will need to decide if it targets only U.S. military facilities in Japan, attacks Japanese critical infrastructure that supports these facilities, or disrupts some broader range of targets. Moving up this target ranking risks expanding and prolonging any conflict, so China may—if it is reasonable (though participants in a conflict tend to become less reasonable the longer it continues)—minimize cyber actions against Japan. The most likely outcome is that in the context of armed conflict, China will decide it has little to lose by launching cyberattacks against Japan's military and critical energy and communications infrastructures and will seek to maximize disruption.

One assumption behind this analysis is that economic warfare (e.g., striking targets in order to degrade the opponent economy and industrial capacity as opposed to striking targets that directly support military operations in order to disrupt them) is unlikely. Although some argue that China has engaged for decades in long-term, low-level economic warfare, this assertion is unsupported by any direct

evidence and Chinese intentions are best described as espionage to build its economy and technological capabilities. In a short conflict, the military benefits of economic warfare would arrive too late to change the outcome and striking civilian manufacturing targets (such as factories) risks expanding the conflict. Although there could be benefits to disrupting production at oil refineries or semiconductor fabs, this benefit is smaller than in the past given the globally distributed nature of supply chains, which creates a fair degree of resilience.

Cyberattacks are most effective when combined with other weapons, including conventional delivery systems, PGMs, unmanned aerial vehicles, and electronic warfare (EW). This combination can cripple command networks and advanced weapons systems and, if done at scale, may overwhelm defenders by exploiting a rapid pace and large scale of action. Against Taiwan, the United States should expect to see a combination of cyber and kinetic attacks. Coordinated kinetic and cyber action against targets in the United States are very unlikely (with the exception of Guam, which is within easy missile range of China). Kinetic actions against targets in the continental United States or Hawaii would create an unmanageable risk of escalation for China.

Influence Operations

Disruption of critical infrastructure may not be the only target of Chinese cyber efforts. China could use its **trove of personal information** on millions of U.S. officials, civilians, and service members to send intimidating or confusing emails, text messages, and social media posts to them and their families (as the Russians have done in Ukraine). Officials in one Asian country have said that China used its access to telecommunications systems in that country to send politically oriented text messages to all mobile phone users in the country and something similar could be done to Americans.

Russia attempted to blend cyberattack, EW, and psychological operations in its invasion of Ukraine. Russian EW systems (such as the **Leer 3**) were able to connect to Ukrainian mobile telephone networks, both to disrupt communications and to collect and send messages. These have had limited success in Ukraine given the political circumstances. The Chinese have not shown the skill of the Russians in influence operations, but the population of Taiwan will be a target for text, email, and video messages—perhaps generated by new artificial intelligence tools—intended to create confusion and emphasize the futility of resistance. The United States should also expect Chinese actors with a presence on U.S. social media platforms to plant disinformation aimed at U.S. media and audiences. China will also try to inject disinformation into global media about U.S. losses and (if there is opportunity) collateral damage to civilian targets from U.S. actions. Artificial intelligence provides a way not only to make more convincing digital falsehoods, but also to inject them at speed and at scale against the target population.

> *The Chinese have not shown the skill of the Russians in influence operations, but the population of Taiwan will be a target for text, email, and video messages—perhaps generated by new artificial intelligence tools—intended to create confusion and emphasize the futility of resistance.*

A global audience, some of which is inherently hostile or predisposed to distrust the United States, is a better venue for China's influence operations than the United States given the broad consensus among **the American population** and leaders on the need to compete with China and the intense reactions that attacks on U.S. territory have generated in the past. The United States cannot assume that Chinese aggression against Taiwan will be met with universal disapproval. Russian propaganda about Ukraine has been successful in Africa, the Middle East, and Latin America despite clear evidence of its aggression. China could similarly engage these audiences. A Chinese campaign could attempt to exploit pacifist sentiment in Asian countries like Japan, but if China is seen as the aggressor, it will likely not gain traction with regional audiences. This suggests that Chinese influence operations will be unsuccessful with U.S. and Northeast Asian audiences but more persuasive in the Global South.

Reconnaissance Is a Warning, Not Necessarily a Prelude

These are likely targets and this analysis does not consider the effect of cyberattacks, which may be limited even if successful, particularly if ships, satellites, aircraft, and air defenses are well defended. However, given the complexity of digital networks and the unevenness of cybersecurity preparation in the United States, if China decides to attack critical infrastructure, some attacks would be likely to succeed. Efforts to create a "zero threat architecture" are misleading in the context of military action by state actors. There will always be some success for cyberattacks, so the goal should be not to prevent but to minimize these successes and to be resilient in the continued provision of digital services when defense inevitably has failed. A later white paper will discuss defending against cyber actions during armed conflict, but planning must consider how to continue necessary operations and services despite cyber disruption.

Conducting reconnaissance is not always a prelude to attack. Russia has conducted strategic reconnaissance against the United States for decades without acting on it. Reconnaissance is, however, an indication of both increased risk and opponent intentions that should guide U.S. preparations for defense. It should be assumed that some percentage of Chinese cyberattacks against U.S. targets would succeed, making the issue a matter of how to ensure resilience and recovery. Even if Chinese cyberattacks against U.S. critical infrastructure are unlikely, the United States needs to prepare for them, improve cyber defenses for the most probable targets, and test its capacity for response and recovery. ■

James A. Lewis *is senior vice president, holds the Pritzker Chair, and directs the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.